



NHSMUN

National High School Model United Nations

Table of Contents

A Note on the NHSMUN Difference.....	3
Position Paper Requirements.....	4
Committee History.....	5

Topic A: The Situation in Nigeria.....6

Introduction.....	7
History and Description of the Issue.....	8
Current Status.....	15
Bloc Analysis.....	23
Committee Mission.....	25

Topic B: Peace and Security in the Age of Cyber Warfare.....26

Introduction.....	27
History and Description of the Issue.....	28
Current Status.....	36
Bloc Analysis.....	42
Committee Mission.....	45

Research and Preparation Questions.....	47
Important Documents.....	48

A Note on the NHSMUN Difference

Esteemed Faculty and Delegates,

Welcome to NHSMUN 2027! We are Armen Bagdassarian and Sabeeh Mirza, and we are elated to serve as this year's Secretaries-General. Thank you for choosing to attend NHSMUN, the world's largest and most diverse high school Model United Nations conference. As a space for collaboration, consensus, and compromise, NHSMUN strives to transform today's brightest thinkers, speakers, and collaborators into tomorrow's leaders. We believe that an emphasis on education through simulation is paramount to the Model UN experience.

Realism and Accuracy: Although a perfect simulation of the UN is never possible, we believe that one of the core educational responsibilities of MUN conferences is to educate students about how the UN System works. We strive to invite real UN, NGO, and field experts into each committee through our committee speakers program. Moreover, we arrange meetings between students and the actual UN Permanent Mission of the country they are representing. These exclusive resources are only available due to IMUNA's formal association with the United Nations Department of Global Communications and consultative status with the Economic and Social Council. No other conference goes so far to deeply immerse students into the UN System.

Educational Emphasis: At the heart of NHSMUN lies education and compromise. Part of what makes NHSMUN special is its diverse delegate base. As such, when NHSMUN distributes awards, we strongly de-emphasize their importance in comparison to the educational value of Model UN. In particular, our daises look for and promote constructive leadership and diplomacy that strive toward consensus, as real ambassadors do in the United Nations.

Research and a Dedicated Staff: Our staffers care deeply about delegates' experiences and what they take away from their time at NHSMUN. Our Directors spend over six months preparing Background Guides, in addition to Update Briefs written to reflect the rapidly changing nature of the topics to be discussed. Our staffers are trained rigorously to provide the best conference experience possible. Our daises provide thoughtful comments on submitted position papers. Our staff aims to tailor the committee experience to delegates' reflections and research, but also to facilitate an environment where all delegates' thoughts can be heard.

Empowering Participation: The UN relies on the voices of all of its member states to create resolutions. This is our philosophy at NHSMUN too. Our Rules of Procedure and our staff focus on making every voice in the committee heard, regardless of country assignment or skill level. Additionally, unlike many other conferences, we also emphasize delegate participation after the conference. Delegates spend countless hours researching topics critical to the UN and broader international sphere.

Delegates, it is our sincerest hope that your time at NHSMUN will be thought-provoking and stimulating. NHSMUN is an incredible time to learn, grow, and embrace new opportunities. We look forward to seeing you work both as students and global citizens at the conference.

Best,

Armen Bagdassarian
Secretary-General

Sabeeh Mirza
Secretary-General

Position Paper Requirements

Delegate research and preparation is a critical element of attending NHSMUN and enjoying the debate experience. We have provided this Background Guide to introduce the topics that will be discussed in your committee. We encourage and expect each of you to critically explore the selected topics and be able to identify and analyze their intricacies upon arrival to the conference.

The task of preparing for the conference can be challenging. To assist delegates, we have updated our [Beginner Delegate Guide](#) and [Advanced Delegate Guide](#). These guides contain more detailed instructions on how to prepare a position paper and excellent sources that delegates can use for research. Use these resources to your advantage. They can help transform a sometimes overwhelming task into what it should be: an engaging, interesting, and rewarding experience.

To accurately represent a country, delegates must be able to articulate its policies. Accordingly, NHSMUN requires each delegation (the one or two delegates representing a country in a committee) to write a position paper for each topic on the committee's agenda. More information about how to write and format position papers can be found in the [Research Guide](#). To summarize, position papers should be structured into three sections.

I: Topic Background – This section should describe the history of the topic as it would be described by the delegate's country. Delegates do not need to give an exhaustive account of the topic, but rather focus on the details that are most important to the delegation's policy and proposed solutions.

II: Country Policy – This section should discuss the delegation's policy regarding the topic. Each paper should state the policy in plain terms and include the relevant statements, statistics, and research that support the effectiveness of the policy. Comparisons with other global issues are also appropriate here.

III. Proposed Solutions – This section should detail the delegation's proposed solutions to address the topic. Descriptions of each solution should be thorough. Each idea should clearly connect to the specific problem it aims to solve and identify potential obstacles to implementation and how they can be avoided. The solution should be a natural extension of the country's policy.

Each topic's position paper should be **no more than 10 pages long** double-spaced with standard margins and 12 point font size. This is a maximum; **3–5 pages per topic is often a suitable length**. The paper must be written from the perspective of your assigned country and should articulate the policies you will espouse at the conference.

Each delegation is responsible for submitting position papers on or before **February 26, 2027**. If a delegate wishes to receive detailed feedback from the committee's dais, their position paper must be submitted on or before **February 5, 2027**. The papers received by this earlier deadline will be reviewed by the committee dais and returned before February 26. Instructions on how to submit position papers will be shared directly with faculty advisors.

Submission instructions for position papers will be sent to faculty advisers via email. If delegations are unable to submit their position papers on time, please contact us at nhsmun@imuna.org.

Delegations that do not submit position papers will be ineligible for awards.

Committee History

The United Nations Security Council (UNSC) was created in 1945 through the UN Charter as one of the six main organs of the United Nations. It was established with the primary responsibility of maintaining international peace and security. Since its first meeting on January 17, 1946, the Security Council has been housed at the United Nations Headquarters in New York City but has held sessions in other cities.¹ The Council comprises 15 members – 10 non-permanent and five permanent members. The five permanent members are known as the P5, which includes China, France, Russia, the United Kingdom, and the United States.² The ten non-permanent members are allocated based on a geographic representation quota and serve two-year terms each. The seat breakdown is as follows: five for African and Asian states, one for Eastern European States, two for the Latin American and Caribbean States, and two for Western European and other States.³ Currently, these include Bahrain, Colombia, Democratic Republic of the Congo, Denmark, Greece, Latvia, Liberia, Pakistan, Panama, and Somalia.⁴

Each member of the Security Council has one vote. An affirmative vote of nine members passes resolutions in the Security Council. However, only the P5 possesses the unique “right to veto” any resolution. If a P5 member votes “no” to a presented resolution, veto power is activated, and the resolution fails automatically.

The Security Council has passed 2,827 resolutions thus far. These resolutions focus mainly on the peaceful resolution of international disputes through negotiations and arbitration.⁵ Peacekeeping missions are one of the Council’s most visible forms of conflict management. These missions work to protect civilians, facilitate political processes, promote human rights, and more.⁶ Since the establishment of the UNSC, over two million peacekeepers from 125 countries have served in 71 peacekeeping missions.⁷ Unlike the General Assembly, decisions made by the Council are legally binding and must be carried out by member states. According to Chapter VII of the UN Charter, the Security Council can enforce its decisions by imposing economic sanctions, ordering an arms embargo, or enacting military action.⁸

¹ “What is the Security Council?” United Nations Security Council, last accessed September 21, 2024, <https://www.un.org/securitycouncil/content/what-security-council>.

² “The UN Security Council,” Council on Foreign Relations, last accessed September 21, 2024, <https://www.cfr.org/backgrounder/un-security-council>.

³ “FAQ Security Council,” United Nations, last accessed September 21, 2024, <https://www.un.org/securitycouncil/content/faq>.

⁴ United Nations Security Council. “What is the Security Council?”/United Nations Official Website. Security Council. 2020. <https://main.un.org/securitycouncil/en/content/current-members>.

⁵ Council on Foreign Relations, “The UN Security Council,” “Resolutions Adopted by the Security Council in 2024 Security Council,” United Nations, last accessed September 21, 2024, <https://main.un.org/securitycouncil/en/content/resolutions-adopted-security-council-2024/>.

⁶ “Maintain International Peace and Security,” United Nations, last accessed September 21, 2024, <https://www.un.org/en/our-work/maintain-international-peace-and-security>.

⁷ “UN Peacekeeping,” Better World Campaign, last accessed September 21, 2024, <https://betterworldcampaign.org/un-peacekeeping>.

⁸ “Security Council,” United Nations, last accessed September 21, 2024, <https://www.un.org/en/model-united-nations/security-council>.

TOPIC A

The Situation in Nigeria

UNSC-B | NHSMUN 2027



Introduction

Nigeria has experienced political, ethnic, religious, and socioeconomic tensions since gaining independence from the United Kingdom on 1 October 1960.¹ Government corruption, uneven access to resources, poverty, and distrust of public institutions continue to affect many communities.² These conditions have been especially severe in northern Nigeria, where unemployment is higher and access to public services is more limited than in southern regions.³ Religious identity is also geographically divided, as Muslims live mostly in the north, Christians reside largely in the south, and the central states known as the Middle Belt include both significant Muslim and Christian populations.⁴

Boko Haram emerged in response to civil dissatisfaction. It evolved into a militant group that has carried out attacks against civilians, schools, religious institutions, political figures, and government forces.⁵ The Nigerian government has consistently tried to mitigate the group with military and police forces, and intelligence personnel such as the Joint Military Task Force (JTF).⁶ However, the same forces intended to protect civilians have also been accused of arbitrary arrests, torture, extrajudicial killings, enforced disappearances, and other human rights violations.⁷

By 2025, Nigeria's security crisis was precarious. Boko Haram's Jama'atu Ahlis Sunna Lidda'awati wal-Jihad (JAS) faction resurged and renewed deadly attacks against civilians in Borno State, while the Islamic State West Africa Province (ISWAP) continued targeting military personnel and bases.⁸ In the northwest, armed criminal groups unaffiliated with either terrorist organization have carried out killings, kidnappings for ransom, and village raids.⁹ In the north-central region, Muslim herding and Christian farming communities compete over land, water, grazing routes, and political influence, sometimes in violent clashes.¹⁰ These varied threats stretch military and governmental personnel and resources, as do the more than two million people displaced by the northeastern insurgency alone.¹¹

Instead of receiving much needed humanitarian

assistance, sometimes civilians face further violations. Government forces have sometimes failed to distinguish between armed insurgents and civilians during counterterrorism and anti-banditry operations. Military airstrikes have fallen indiscriminately, civilians have been detained and tortured for information, and police and other security personnel have been accused of demanding bribes and extorting civilians.¹²

The conflict is important to the United Nations Security Council (UNSC) because its effects extend beyond Nigeria's borders. Boko Haram and ISWAP have additionally operated in Cameroon, Chad, and Niger.¹³ These armed groups move fighters, weapons, and supplies across national borders. The violence has also displaced civilians, disrupted education and food production, restricted humanitarian access, and weakened regional security.¹⁴ Political tensions among Lake Chad Basin states have affected collaboration and information-sharing.¹⁵ The UNSC must therefore consider how to support Nigeria and neighboring states, restore regional cooperation, and protect civilians.

History and Description of the Issue

CONDITIONS BEHIND THE CONFLICT

Nigeria is located in Western Africa and shares a coastline with the Gulf of Guinea in the Atlantic Ocean.¹⁶ It is bordered by Benin and Cameroon, Chad, and Niger in the Lake Chad basin. The Nigerian government recognizes approximately 250 ethnic groups living in the country, including the Hausa, Igbo, and Yoruba.¹⁷ In Nigeria, colonial borders forced separate ethnic groups together into single countries while simultaneously splitting unified groups apart. These artificial arrangements created longstanding differences, inequalities, and disagreements, compounded by contemporary religious divides.

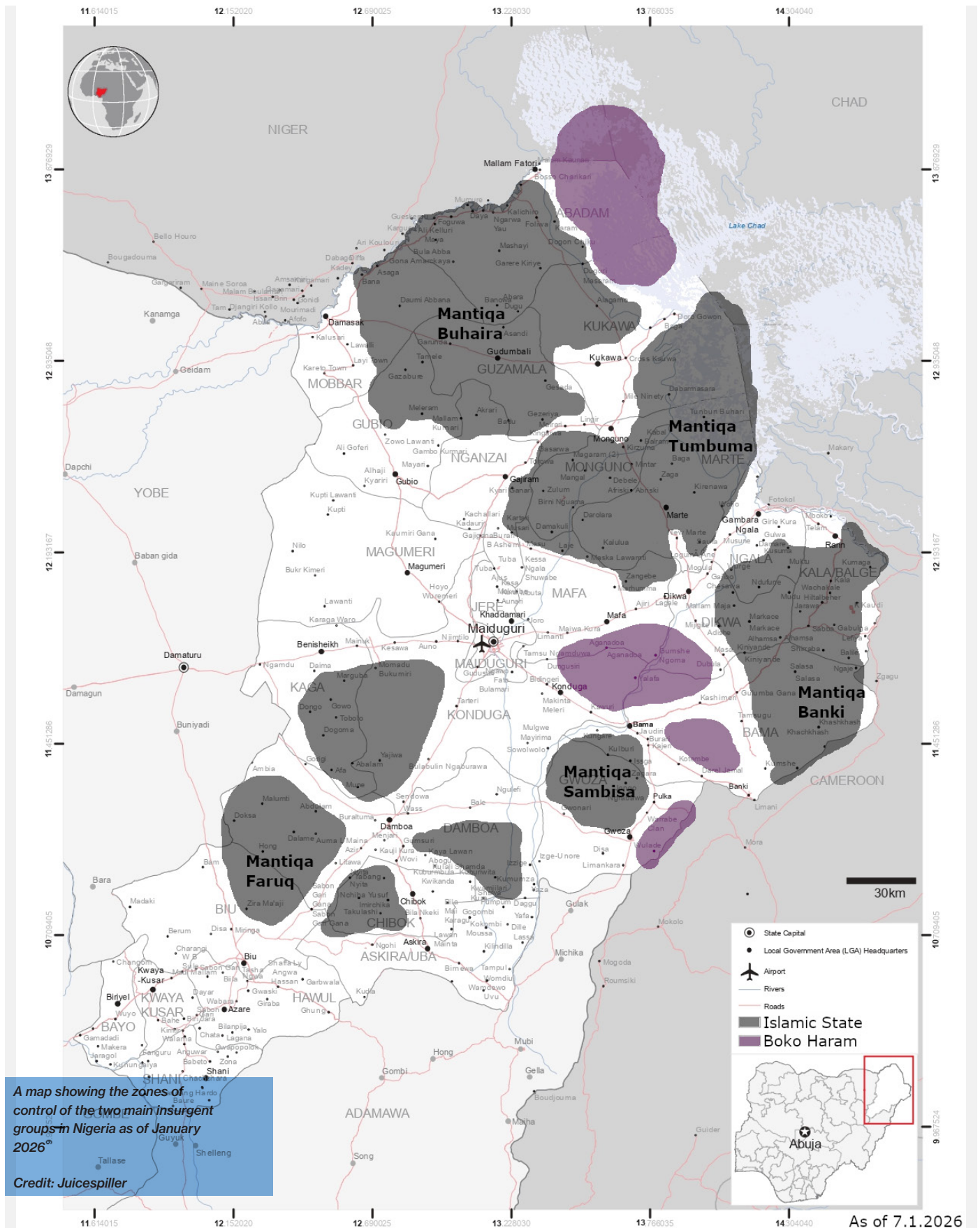
Islam and Christianity are currently the two most dominant religions practiced in the country.¹⁸ Muslims live mostly in northern Nigeria, while Christians reside mainly in southern Nigeria. The Middle Belt includes a more balanced number of Muslims and Christians living together.¹⁹ Islam became established in northern Nigeria through trade, migration, and scholarship. It then became closely connected to political authority under the Sokoto Caliphate.²⁰ Christianity spread more widely in southern Nigeria during the nineteenth century, particularly through missionary activity under British colonial rule.²¹ These different historical patterns contributed to the country's present religious geography, although neither northern nor southern Nigeria are religiously uniform.

From Nigeria's independence in 1960 to 1998, it experienced an era of political turmoil with various coups, different military leaders as political rulers, and a three-year civil war.²² The 1998 death of General Sani Abacha, the final military leader to hold a monopoly on political power, allowed Nigeria to hold parliamentary and presidential elections and thus put an end to military rule in 1999.²³ Religious violence

increased after Nigeria returned to democratic rule in 1999 since there was no longer a military government to tightly restrict political activity.²⁴ Democracy created greater political freedom and competition, but also allowed existing religious tensions to become more openly connected to elections, laws, and struggles over government power. Intercommunal violence has been especially deadly in the Middle Belt, with many "tit-for-tat killings" based on ethnic or religious identities.²⁵ Economic dissatisfaction, political grievances, and social strife also contribute to communal and sectarian violence.²⁶

Corruption in Nigeria has diverted public resources away from essential services like infrastructure development. It has also contributed to poverty and weakened public trust in the Nigerian government.²⁷ The country has consistently ranked high on Transparency International (TI)'s Corruption Perceptions Index (CPI).²⁸ Many public officials engage in corruption because the temptation for extra benefit is too great and the threat of simple jail time is not dissuasive enough.²⁹ As a result, Nigeria's economic growth has been economically hampered. Although it is a top crude oil producer and exporter, corruption and the mismanagement of natural resources have enriched individuals instead of supporting public programs. Additionally, some funds allocated for counterinsurgency operations in Nigeria are directly diverted for personal gains.³⁰ Limited funding can lead to inadequate military preparedness, low troop morale, a lack of essential resources, and less effective security measures.

Corruption has also affected the operations of the country's police forces and justice system. Nigerian police have been accused of demanding money from victims before initiating investigations and from suspects during criminal proceedings.³¹ Other police officers also may not have adequate resources to protect the public, due to embezzlement. Former U.S. Secretary of Defense Robert McNamara argued that "any society that seeks to achieve adequate security



A map showing the zones of control of the two main insurgent groups in Nigeria as of January 2026⁹

Credit: Juicespiller

against the background of acute poverty has a false sense of security,” which helps to explain Nigeria’s continuing security challenges.³² This history has eroded much public trust in government institutions, which created an opportunity for other forces like Boko Haram to gain support as an opposition to government corruption and abuses.

Poverty is disproportionately concentrated in northern Nigeria, where Boko Haram is centralized. According to Nigeria’s 2022 Multidimensional Poverty Index, approximately 86 million of the country’s 133 million multidimensionally poor people lived in the northern regions.³³ Communities in the north have experienced higher unemployment, less access to resources, and greater disparities in wealth.³⁴ These economic struggles increase dissatisfaction with the government and more openness to other options.

Recognizing the situation, the Nigerian government has aimed to address the military’s limited resources and low morale. In August 2026, the presidency announced salary increases ranging from 30 to 80 percent for thousands of soldiers.³⁵ This was the largest military pay increase in years, and is a hopeful start in improving the armed forces’ struggle against concurrent insurgencies across the state. Improved pay may strengthen recruitment, retention, and morale, but it does not address allegations of abuse, weak oversight, or impunity. Therefore, Nigeria, its neighbors, and the wider UNSC continue to struggle with how to address the security crisis in the country.

THE ORIGINS AND EXPANSION OF BOKO HARAM

In 2002, Boko Haram formed under the leadership of Mohammed Yusuf in a remote area of Yobe State.³⁶ The group was known as Al Sunna wal Jamma, or the Nigerian Taliban, during this period. It was made up of many university students, unemployed youth, and refugees from the Lake Chad region who were frustrated with socioeconomic conditions in Nigeria and supported Yusuf’s teachings.³⁷ The group had two central aims. The first was to withdraw from the Nigerian state, which it viewed as corrupt, unjust, sinful, and influenced by Western education; the second was to establish a new state in northern Nigeria based on Islamic law.³⁸ Originally, Boko Haram established mostly peaceful systems for providing welfare, food, and shelter to attract more followers.³⁹

Shortly after settling in the northern state of Yobe, the group’s members began to dispute with local residents and government authorities after the extremist commune was allegedly attempting to establish a “state within a state.”⁴⁰ Police issued an eviction notice, which the group labeled as religious persecution.⁴¹ In relation, members attacked police stations in Kanamma and Damaturu in December 2003.⁴² The Nigerian government then deployed military forces to completely remove the group from the region. Although Yusuf fled to Saudi Arabia to avoid arrest, he later returned to Nigeria and continued preaching. Nigerian authorities arrested him several times between 2008 and 2009.⁴³

Tensions culminated in a July 2009 uprising

Communities in the north have experienced higher unemployment, less access to resources, and greater disparities in wealth.

across several northern states. Nigerian security forces killed hundreds of people and captured Mohammed Yusuf, who was subsequently executed in police custody.⁴⁴ Although the government initially believed the movement had been defeated, Boko Haram reorganized underground and re-emerged under Abubakar Shekau in 2010.⁴⁵

This movement formally became known as Jama'atu Ahlus-Sunnah Lidda'Awati Wal Jihad, or People Committed to the Propagation of the Prophet's Teachings and Jihad.⁴⁶ The group changed its capabilities and tactics during this period. Previously, it focused primarily on local politicians accused of corruption. Then, it began to target the Nigerian government and members of the population who did not follow its interpretation of Islam, especially Christians.⁴⁷ The group became increasingly dangerous as it caused more civilian deaths, developed more sophisticated tactics, and established relationships with other militant organizations.

In the international community, the group became known as Boko Haram, a name commonly translated as "Western education is forbidden" or "Western education is a sin."⁴⁸ Boko Haram subsequently made education a central target

of its insurgency. The insurgents have attacked schools, killed teachers and students, and abducted schoolchildren.⁴⁹ These attacks have expanded from northeastern Nigeria into neighboring countries throughout the Lake Chad Basin.

From July 2009 to October 2012, Boko Haram killed an estimated 1,500 people in northern and central Nigeria.⁵⁰ After approximately 200 members were killed during the July 2009 confrontation with security forces, Boko Haram began a broader campaign of violence and sought technical and financial assistance from al-Qaeda in the Islamic Maghreb.⁵¹ This assistance was provided. President Goodluck Jonathan declared a state of emergency, but the emergency powers granted to government security forces failed to eliminate the threat.⁵²

Boko Haram's official operations eventually expanded beyond Nigeria into Cameroon, Chad, and Niger. Nigeria and its neighbors responded through creating the Multinational Joint Task Force (MNJTF), which launched regional counterinsurgency operations.⁵³ Internal divisions also changed Boko Haram. In 2016, the Islamic State announced Abu Musab al-Barnawi as the leader of its West African branch.⁵⁴ Abubakar

Nigerian soldiers perform a military demonstration near Boko Haram territory as a show of strength.

Credit: VOA/Nicolas Pinault



Shekau rejected the decision, contributing to a split between factions commonly described as Boko Haram (JAS) and the Islamic State West Africa Province (ISWAP).⁵⁵

BOKO HARAM'S ATTACKS ON CIVILIANS AND CIVILIAN INFRASTRUCTURE

Boko Haram has been accused of committing widespread and systematic attacks against civilians. The group has targeted people it considers “unbelievers,” including Christians, local politicians, community leaders, and any Muslims perceived as opposing its mission.⁵⁶ Boko Haram has organized attacks in public spaces such as schools, markets, villages, and religious buildings.⁵⁷ In fact, the group’s actions have been so severe that the Office of the Prosecutor of the International Criminal Court concluded that there was a reasonable basis to believe Boko Haram had committed war crimes and crimes against humanity since July 2009.⁵⁸

The faction most frequently called “Boko Haram” is formally known as Jama’atu Ahlis Sunna Lidda’awati wal-Jihad (JAS), while its principal rival is the Islamic State West Africa Province (ISWAP).⁵⁹ Their disagreement is partly rooted in differences over governance and the treatment of civilians. JAS frequently kills, abducts, and steals from civilians, including Muslims, while ISWAP generally seeks to control Muslim communities by collecting taxes and enforcing its own laws.⁶⁰ However, it also uses violence against civilians who resist its authority or cooperate with the government.⁶¹ ISWAP uses coercion, targets people it considers disloyal, and places significant pressure on communities under its influence.

ISWAP has frequently concentrated its operations on Nigerian military forces and infrastructure. Between 2017 and 2019, the faction attacked or overran several military positions in Borno State, including bases in Metele, Baga, Gubio, Marte, and Kirenowa.⁶² These attacks killed soldiers, forced troops to withdraw, and allowed ISWAP to seize

weapons and other supplies. In December 2018, ISWAP captured the commercial town of Baga and overran a nearby base operated by the Multinational Joint Task Force, the cooperative force that Cameroon, Chad, Nigeria, Benin, and Niger (at the time) participated in.⁶³

Before the movement formally split into JAS and ISWAP in 2016, Boko Haram frequently used improvised explosive devices and suicide bombings against security forces and civilians.⁶⁴ In December 2010, the group used explosive devices to target the Christian community in Jos, Plateau State, killing approximately 80 people.⁶⁵ It later began using suicide attacks against Nigerian police forces, political figures, religious institutions, and civilians.⁶⁶ The repeated use of these tactics demonstrated the group’s operational capacity for planning and executing coordinated attacks.

In November and December 2011, Boko Haram committed a series of attacks against Christians in Damaturu and other locations.⁶⁷ Previously, Boko Haram had targeted Christians more at random, but these attacks were part of a new campaign to drive Christians from northern communities. This also further attracted publicity through attacks on prominent churches and strengthened Boko Haram’s claim that it was defending Islam against the Nigerian government.⁶⁸ Boko Haram targeted local churches near its bases in Borno and Yobe states, launched bombings against high-profile churches in Plateau State, and conducted smaller operations against Christian communities in northern Nigeria and the Middle Belt.⁶⁹ The group has also targeted Muslims who rejected its interpretation of Islam or opposed its political objectives.⁷⁰

Boko Haram has carried out several mass killings. During the Baga massacre in January 2015, their attacks may have killed as many as 2,000 people in and around the town.⁷¹ Boko Haram also burned homes, destroyed vegetation and personal property, and displaced thousands of residents. In January 2019, the group attacked



Remains of a destroyed MT-LB armored vehicle stolen from Nigerian forces by ISWAP and then destroyed in combat

Credit: Jambanja2009

Rann in Borno State, killing approximately 60 people by setting houses on fire and attacking individuals who attempted to flee.⁷² These attacks show a continuing pattern of mass violence intended to kill civilians, displace people, and destroy infrastructure.

As reflected in their name, schools have also been central targets. In February 2012, the group began targeting schools around Maiduguri in Borno State, setting twelve schools on fire within a two-week period.⁷³ By destroying school property and creating fear among students and teachers, Boko Haram has consistently disrupted education throughout northeastern Nigeria. In a highly covered case, Boko Haram abducted 276 girls from a secondary school in Chibok, Borno in April 2014.⁷⁴ Girls who escaped reported that they had been forced to marry their captors and had experienced sexual abuse in Boko Haram camps.⁷⁵ More than a decade after the Chibok abduction, at least 91 of the girls remained in captivity or their fate was unknown.⁷⁶ Overall, the year 2014 was especially violent. Nigeria experienced a significant increase in terrorist activity that year with 7,512 deaths, an increase of over 300 percent since 2013.⁷⁷

In February 2018, Boko Haram abducted 110 schoolgirls from the Government Girls Science and Technical College in Dapchi, Yobe State.⁷⁸ The following month, Boko Haram abducted three humanitarian workers during another attack that killed dozens of people.⁷⁹ The group has also been accused of recruiting children as soldiers and using children, especially girls, as suicide bombers.⁸⁰ Protecting civilians in Nigeria requires protecting schools and humanitarian operations, preventing child recruitment, and securing the release and reintegration of abducted children.

Conflict between JAS and ISWAP has created additional risks for civilians. The leader of Boko Haram (JAS) Abubakar Shekau died in 2021, after which ISWAP initially appeared likely to become the dominant faction.⁸¹ However, JAS later regained territory, capturing most of the Lake Chad islands previously controlled by ISWAP during 2023. Although fighting between the factions has killed many of their own combatants, it has not eliminated either organization. JAS's territorial gains exposed more civilians around Lake Chad and the Mandara Mountains to killing, abduction, and looting, while ISWAP continued to tax and pressure communities in central Borno

and eastern Yobe State.⁸²

These attacks force civilians to leave their homes, prevent children from attending school, interrupt farming and local trade, and make humanitarian assistance more difficult to deliver. For the UNSC, the central concern is how the group's organized violence threatens civilian populations and contributes to instability throughout Nigeria and the wider Lake Chad Basin.⁸³ The factions may require different international responses. JAS relies heavily on raids, looting, and kidnapping for ransom, while ISWAP obtains revenue through both kidnapping and a more organized taxation system imposed on communities and economic activity under its control.⁸⁴

GOVERNMENT COUNTERINSURGENCY AND ALLEGED SECURITY-FORCE ABUSES

The Nigerian government has responded to Boko Haram's violence by deploying government security forces. The Joint Military Task Force, which contains military, police, and intelligence personnel, is also active in the area.⁸⁵ The JTF is usually deployed to conduct counterinsurgency operations after Boko Haram attacks. Although these forces were sent to protect the public and combat the insurgency, they have also been accused of committing serious human rights violations.⁸⁶

Security forces frequently conducted community raids during the earlier years of the insurgency.⁸⁷ This usually happens after Boko Haram has already attacked. Human Rights Watch

documented allegations that security personnel arbitrarily arrested and beat residents, searched civilian homes, stole money, and burned houses, shops, and vehicles.⁸⁸ Witnesses also reported that security forces executed men outside their homes or businesses, sometimes in front of their families. Many suspected Boko Haram members were subsequently held without charges or trials for months or years in police and military detention facilities. There, detainees were reportedly subjected to physical abuse, torture, and extrajudicial killing.⁸⁹ Torture has reportedly been used to punish or humiliate detainees and to obtain confessions from people suspected of supporting Boko Haram.

Recent research suggests that security-force abuse has continued beyond the insurgency's early years. A 2025 qualitative study interviewed displaced victims of terrorism living in IDP camps about their experiences with Nigerian security personnel.⁹⁰ These participants in Borno State described physical and psychological abuse, sexual violence, economic exploitation, and torture.⁹¹ These testimonies indicate that concerns about abusive counterterrorism operations continue into the present.

Civilian-protection concerns extend to Nigeria's increasing reliance on airstrikes. In 2026, a Nigerian military airstrike intending to target armed groups at a market in Zamfara State reportedly killed at least 100 civilians.⁹² High civilian casualty totals in this and other attacks have raised concerns about target identification, proportionality, and precautions taken before attacks. Civilians may face danger from both armed groups and the government operations

In 2026, a Nigerian military airstrike intending to target armed groups at a market in Zamfara State reportedly killed at least 100 civilians.

intended to protect them. Although JAS and ISWAP take up much attention, the actions of those attempting to counteract the insurgents also require scrutiny.

Enforced disappearances present another concern. After community raids, security forces have arrested thousands of suspected Boko Haram members and transferred them to military detention centers.⁹³ It is difficult to determine how many people have been detained or where they are being held because Nigeria historically lacks a centralized system for recording arrests. Amnesty International identified approximately 1,200 people arrested between 2011 and 2014 whose families did not know their whereabouts.⁹⁴ Children have also been detained on suspicion of association with Boko Haram, sometimes with little or no evidence, and without contact with their families.

More recent operations demonstrate that Nigerian security forces can also play an essential role in protecting civilians. In August 2026, a joint intelligence-led operation involving the military, police, and counterterrorism units rescued 308 people held in the forests of Kainji Lake National Park.⁹⁵ Officials described the operation as intelligence-led, but did not disclose the source of the intelligence or how the rescue was conducted.⁹⁶ The rescued civilians included 163 people abducted during an attack on Woro in Kwara State and 145 people taken primarily from neighboring Niger.⁹⁷ Officials reported that survivors received medical evaluations at an army facility before being reunited with their families.

Effective, intelligence-led operations can strengthen civilian confidence in Nigerian security institutions.⁹⁸ Conversely, abusive or indiscriminate operations may weaken the government's counterinsurgency campaign. When security forces commit violence against the communities they are meant to protect, residents may become less willing to cooperate or provide information.⁹⁹ Government abuses can also support Boko Haram's claim that the Nigerian state is corrupt and unjust.

Current Status

RESURGENCE AND EXPANSION OF ARMED VIOLENCE

Nigeria recorded nearly 12,000 conflict-related deaths in 2025 according to one source.¹⁰⁰ This total exceeds the peak fatalities recorded during the height of the Boko Haram insurgency in 2014 and more than those suffered in Iraq, Syria, and Yemen combined in 2025.¹⁰¹ Since January 2025, ISWAP has launched coordinated offensives against military positions in Borno and Yobe states, attacking more than a dozen bases and other military targets.¹⁰²

One example of these attacks occurred on 7 July 2026, when suspected ISWAP fighters launched a coordinated attack on a Forward Operating Base in Logomani, Ngala Local Government Area of Borno State.¹⁰³ The attackers briefly breached part of the base's defensive perimeter, killing one soldier and damaging two gun trucks and other military equipment. Nigerian troops regrouped and forced the attackers to retreat. More government reinforcements were deployed, and a combined security team pursued the fleeing insurgents. The militants also entered the surrounding community and burned a police outpost, a primary healthcare center, and two classrooms.¹⁰⁴ This incident demonstrated ISWAP's continuing ability to organize coordinated assaults on military positions while also threatening civilian infrastructure in frontline communities.

In several cases, insurgents have temporarily overran isolated positions, killed soldiers, and seized weapons or other supplies before withdrawing or facing government reinforcements.¹⁰⁵ ISWAP has retained substantial intelligence, mobility, weapons, and command capabilities, despite earlier territorial losses. In March 2026, ISWAP also overran four military bases during two days of attacks and killed dozens of Nigerian soldiers.¹⁰⁶ Boko Haram's JAS faction has also continued attacking civilian

communities.¹⁰⁷

Violence in northeastern Nigeria increased in intensity and sophistication during 2025. ISWAP has escalated its operations, using coordinated nighttime assaults and explosive-equipped drones. It has aimed to sabotage infrastructure and isolated military bases.¹⁰⁸ ISWAP's destruction of roads and bridges demonstrate the group's ability to contest rural areas, disrupt military supply routes, and isolate strategically important towns.¹⁰⁹

Following Abubakar Shekau's death in 2021, surviving members of JAS pledged loyalty in May 2022 to a new leader known as Abu Umainata, who has also been named as Bakura Doro.¹¹⁰ Nigerian authorities claimed that he was killed in an August 2025 airstrike, but Boko Haram reportedly denied his death. The faction's current leadership structure therefore remains unclear.¹¹¹

ISWAP is reportedly led by Abu Musab al-Barnawi.¹¹² It also has a governing Shura Council that provides strategic oversight and approves leadership appointments, while formal departments known as dawawin oversee military operations, taxation, religious enforcement, justice, and public welfare.¹¹³ ISWAP regulates

economic activity and collects taxes in areas under its influence, particularly in Borno State and on islands in Lake Chad. This revenue helps purchase weapons, medicines, fuel, and other supplies. Its connection to the central Islamic State organization has also provided access to technical expertise, military advisers, funding, and propaganda support.¹¹⁴

The religious dimensions of the violence became an international controversy in late 2025. United States President Donald Trump accused the Nigerian government of failing to prevent widespread killings of Christians and threatened to suspend assistance or consider military action.¹¹⁵ The United States subsequently designated Nigeria a country of particular concern on religious-freedom grounds. Nigerian officials rejected the characterization of the crisis as a campaign tolerated by the government, emphasizing that extremist and criminal violence affects both Christian and Muslim communities.¹¹⁶ Religious identity can influence who is targeted, but describing all violence as a single religious conflict obscures these overlapping causes and the extensive attacks that Muslim communities have also endured.

On 15 May 2026, armed insurgents riding



Abu Musab al-Barnawi

Credit: The Nigerian Voice

motorcycles entered primary and junior secondary schools in Mussa, Askira/Uba Local Government Area of Borno State, shortly after a military patrol left the community. Local sources reported that the attackers abducted 40 children, including some younger than five.¹¹⁷ The perpetrators were suspected members of either Boko Haram or ISWAP, although responsibility had not been conclusively established. The incident illustrates how insurgents continue to exploit gaps in civilian protection to attack schools and abduct children in communities near the Sambisa Forest.¹¹⁸

On 16 May 2026, a joint Nigerian-United States operation killed Abu-Bilal al-Minuki, a Nigerian militant described by officials as the Islamic State's second-in-command globally.¹¹⁹ According to Nigerian and United States officials, al-Minuki helped coordinate Islamic State operations across several regions and had connections to ISWAP.¹²⁰ His death represented a significant counterterrorism success, but it did not eliminate the networks operating in northeastern Nigeria. Previous leadership deaths and internal conflicts have also temporarily weakened Boko Haram factions without ending their ability to reorganize and conduct attacks.¹²¹

Following these events in July 2026, the United States withdrew most of the approximately 200 personnel deployed to support counterterrorism operations in Nigeria.¹²² That same month, ISWAP attempted to infiltrate Maiduguri and abduct students in Monguno.¹²³ These bold attempts show that despite the success of recent joint operations and the deaths of senior militants, ISWAP retains the capacity to threaten major population centers and conduct abductions.

Jihadist insurgents are only one part of Nigeria's security crisis. Nigerian forces are deployed across much of the country in response to insurgency, banditry, kidnapping, and farmer-herder/communal violence.¹²⁴ Violence in the Middle Belt is often called "farmer-herder clashes," but this description is disputed. Some leaders and communities in Benue and Plateau

argue that it wrongly suggests equal fighting between armed attackers and vulnerable rural communities.¹²⁵ The violence has several causes, including disputes over land, water, and grazing routes, as well as ethnic and religious tensions. In Benue State, violence following the assassination of the chair of a Fulani livestock owners' association reportedly killed at least 57 people and displaced thousands during July 2026.¹²⁶ Although this violence is distinct from the Boko Haram insurgency, it competes for government attention and security resources while contributing to Nigeria's wider displacement crisis.

In northwestern and north-central Nigeria, armed groups commonly described as bandits conduct violent raids, cattle rustling, mass abductions, extortion, and kidnappings for ransom.¹²⁷ Banditry has grown in rural areas affected by poverty and limited economic opportunities as a survival strategy. It thrives under weak government control and inadequate security protection.¹²⁸ Over time, some groups have become more organized, controlling communities, imposing payments, and forcing captives to work.¹²⁹ Bandit groups are generally motivated more by profit rather than the ideological objectives of Boko Haram or ISWAP, but some reports allege that both sides may share weapons, information, or other forms of assistance. These relationships are usually temporary and transactional, and groups that cooperate at one point may later compete or fight.¹³⁰

In June 2026, bandits abducted at least 39 civilians during a community reconciliation meeting in Magamin Diddi, Zamfara State.¹³¹ The meeting had been organized to facilitate dialogue between residents and relatives of a bandit leader.¹³² The leader arrived with armed members of his group and abducted participants. With inadequate state protection, some communities might be desperate enough to negotiate directly with armed groups. However, this leaves residents vulnerable, even during attempts to establish peace.

Kidnapping has become an important source of income for both jihadist organizations and non-ideological armed groups. SBM Intelligence documented at least 7,825 abductions between July 2025 and June 2026, a 66 percent increase over the previous twelve-month period.¹³³

Approximately 80 percent of victims were taken in mass abductions, and at least 1,142 people, including 895 civilians, were killed in kidnapping-related violence.¹³⁴ Although the northwest remained the center of the crisis, major abductions also occurred in northeastern and north-central Nigeria. The true totals may be higher because many victims and families do not report abductions or ransom payments.

These simultaneous security issues stretch Nigeria's personnel and operational capacity. Security forces also face gaps in intelligence, mobility, communications, equipment, and logistical support, which can prevent them from reinforcing isolated positions or responding quickly to attacks.¹³⁵ Insurgents can exploit these weaknesses to disperse, regroup, and regain the initiative. The Nigerian government and its international partners must therefore decide whether to concentrate resources on the northeastern insurgency or strengthen security and civilian-protection capacity across several regions.

CIVILIAN PROTECTION AND THE HUMANITARIAN CRISIS

A 2021 UNDP study estimated that the conflict had caused nearly 350,000 direct and indirect deaths by the end of 2020.¹³⁶ This figure included

deaths caused by the destruction of agriculture, health services, trade, water systems, and other essential infrastructure, not just people directly killed in attacks. Boko Haram's activities have reduced agricultural production, obstructed trade routes, closed local markets, and restricted access to food and water.¹³⁷ These are often purposeful actions, like poisoning water supplies, burning crops, and destroying farming infrastructure. This makes it even harder for civilians to meet their basic needs.

Reports from 2026 indicate that 3.7 million people are internally displaced across Nigeria.¹³⁸ More than 400,000 Nigerians displaced by the northeastern conflict had also sought refuge in Chad, Niger, and Cameroon.¹³⁹ An October 2025 food-security analysis found that 27.2 million people across Nigeria faced acute food shortages, a figure projected to reach 34.8 million by mid-2026.¹⁴⁰ Meanwhile, 5.9 million people in northeastern Nigeria required humanitarian assistance under the 2026 Humanitarian Needs and Response Plan.¹⁴¹ These categories of food insecurity and humanitarian need both demonstrate that the effects of the insurgency extend beyond people directly killed or injured.

Forms of harm against civilians can differ across populations. Women and girls face particular risks of abduction, forced marriage, rape, sexual slavery, and domestic servitude. Boko Haram has also used girls as suicide bombers.¹⁴² Even after escaping captivity, some girls and young women have been unlawfully detained by the Nigerian military because of their real or perceived association with Boko Haram. Survivors may also experience disrupted education, inadequate

27.2 million people across Nigeria faced acute food shortages, a figure projected to reach 34.8 million by mid-2026.



Nigerian refugees in Niger

Credit: EU Civil Protection and Humanitarian Aid

access to healthcare and psychological support, and stigma or rejection from their families and communities.¹⁴³

Children of any gender also may be abducted, recruited or used by armed groups, separated from their families, deprived of education, or detained because of alleged association with insurgents.¹⁴⁴ Farming and herding communities have experienced cycles of attack and retaliation connected to competition over land. Violence has killed and displaced families, destroyed homes, and resulted in livestock being killed, poisoned, or stolen.¹⁴⁵ Because ethnic identities are frequently associated with Christianity or Islam, conflicts rooted in land access or retaliation may also be portrayed as religious violence.¹⁴⁶ Refugees and internally displaced people may face stigma and human-rights violations, limited access to legal remedies, and inadequate access to food, shelter, healthcare, education, water, and sanitation.¹⁴⁷

Displacement can continue long after an area is retaken from militants. Families may be unable to return because their homes, farms, livestock, businesses, and community infrastructure have been destroyed.¹⁴⁸ The area may also be

at risk of future recapture. Displaced people often lack adequate access to food, water, sanitation, shelter, education, and healthcare both while displaced or as they rebuild their lives elsewhere.¹⁴⁹

Closures of refugee or IDP camps can leave displaced people choosing between returning to unsafe communities, moving into overcrowded host communities, or living without reliable assistance.¹⁵⁰ While in camps, displaced communities' land could be reassigned before their claims and right to return are addressed.¹⁵¹ For example, displaced residents from Guma in Benue State have been unable to return safely or access their ancestral land. Their property losses have also not officially been fully recorded.¹⁵² In August 2026, the federal government considered creating ranches in Benue, but community organizations demanded that displaced residents be returned before any land was allocated. New land projects could permanently prevent displaced families from recovering their property.¹⁵³

During reintegration, former captives and those perceived as having lived under armed-group

control may also face additional screening, detention, or community suspicion during the return process. For example, one former captive was held in the forest for nearly seven years and escaped with three children born after she was forcibly married to different fighters.¹⁵⁴ After returning home, she received little rehabilitation or support and was rejected by her family. The rejection was so severe, she considered returning to captivity.¹⁵⁵ Safe and sustainable reintegration solutions thus require access to essential services, legal and institutional protection, and the full participation of displaced people in decisions affecting their return, local integration, or resettlement.¹⁵⁶ Restoring physical security alone is insufficient.

Humanitarian organizations face serious security and financial constraints.¹⁵⁷ Continuing violence, suicide bombings, and the widespread use of improvised explosive devices endanger civilians and impede humanitarian access across northern Nigeria. Funding is also a severe issue. As of 1 September 2026, the 2026 Humanitarian Needs and Response Plan had received only about 69.5 percent of its requested funding, leaving an unmet requirement of approximately USD 157.6 million.¹⁵⁸ These funding shortages have forced humanitarian organizations to concentrate limited resources on the most severe and immediately life-threatening needs. Because of the shortages, Nigeria is taking more responsibility for helping people in crisis. The UN is providing expert support while Nigeria finds more funding from its government and businesses.¹⁵⁹ Even so, civilians in remote and conflict-affected communities may still receive little or no assistance.

Counterterrorism operations may also be necessary to protect communities, but arbitrary detention, torture, enforced disappearance, extrajudicial killing, and indiscriminate force can violate international human rights and humanitarian law.¹⁶⁰ For example, in April 2026, a Nigerian Air Force strike hit a crowded market in Jillli village.¹⁶¹ This reportedly killed approximately 200 civilians. Weeks later, another airstrike reportedly struck the busy Tumfa market in

Zamfara State, killing at least 100 civilians, including many women and girls.¹⁶²

The Security Council must decide how to support counterterrorism operations without increasing civilian harm. To best protect civilians and maintain humanitarian standards, counterterrorism action must consider potential impacts of a blind focus on rooting out all insurgents.¹⁶³ Military assistance could require better intelligence checks, safer targeting procedures, human rights training, detention protections, and credible investigations of alleged abuses.¹⁶⁴ Delegates should also consider how to preserve humanitarian access and ensure that displaced people return voluntarily and safely. If sanctions interfere with humanitarian work, exemptions may be needed so aid organizations can deliver food and medicine while preventing assistance from being diverted to Boko Haram or ISWAP.¹⁶⁵

NATIONAL, REGIONAL, AND INTERNATIONAL RESPONSES

Nigeria retains primary responsibility for protecting people within its territory, but the cross-border operations of Boko Haram and ISWAP make regional and international cooperation necessary. Nigerian forces and the Multinational Joint Task Force (MNJTF), have recaptured territory previously held by Boko Haram, arrested or killed fighters and commanders, and impacted the capabilities of both JAS and ISWAP.¹⁶⁶ More than 100,000 Boko Haram associates and combatants have also reportedly surrendered to government forces.¹⁶⁷ However, these successes have not ended the insurgency. Boko Haram and ISWAP have adapted by conducting hit-and-run attacks and ambushes, shifting their areas of operation when pressured, and exploiting the difficult terrain and islands of the Lake Chad Basin. Boko Haram has also retained control of some territory in the Lake Chad islands and continually threatens Nigeria and neighboring states.¹⁶⁸ Since Nigeria's armed forces are deployed across approximately two-thirds of the country, personnel, equipment, intelligence capabilities, and funding are

stretched thin.¹⁶⁹

The MNJTF includes Nigeria, Benin, Cameroon, Chad, and, until its withdrawal in 2025, Niger.¹⁷⁰ The MNJTF has conducted military and nonmilitary efforts against Boko Haram and ISWAP around Lake Chad. The MNJTF operates under the political authority of the Lake Chad Basin Commission and an African Union Peace and Security Council mandate.¹⁷¹ Its operations are intended to weaken Boko Haram and ISWAP, improve regional military cooperation, and create conditions for stabilization and assistance to affected communities.¹⁷² However, Niger's 2025 withdrawal left a security gap around the Diffa region and disrupted intelligence sharing and military cooperation.¹⁷³

The MNJTF is not a fully integrated army. The national contingents generally operate within their own countries.¹⁷⁴ Governments retain substantial control over their forces; the MNJTF force commander lacks full command and control authority. This structure, combined with limited information sharing and differing national priorities, can complicate joint planning, intelligence sharing, and long-term cross-border operations.¹⁷⁵ Changes in national priorities can weaken the collective responses, such as with

Niger. The country withdrew from the MNJTF in 2025 partly to redeploy forces to protect its oil pipeline to Benin, leaving a security gap around the Diffa region.¹⁷⁶ Political tensions have also disrupted regional intelligence sharing and military cooperation. Meanwhile, Boko Haram and ISWAP recruited new members, regained strength, attacked military bases, and expanded their operations beyond the Lake Chad Basin.¹⁷⁷

Restoring full cooperation in the area would probably require diplomatic engagement with Niger rather than military assistance alone.¹⁷⁸ The Lake Chad Basin Commission and African Union could provide forums for negotiation. However, the UNSC cannot compel any country to participate, but UN bodies have made strong recommendations. The UNHCR has called for coordinated border monitoring, early-warning systems, emergency preparedness, and protection responses across Cameroon, Chad, Niger, and Nigeria.¹⁷⁹ It also requested approximately USD 29 million for these regional humanitarian and protection efforts between June and December 2026.¹⁸⁰ This cross-border effort could address both immediate civilian needs and the conditions that allow insecurity to persist.

MNJTF partners planning a training exercise in 2017

Credit: US Army Capt. Jason Welch



The Security Council has addressed the conflict through Resolution 2349 of 2017, its first resolution focused specifically on the Lake Chad Basin crisis.¹⁸¹ The resolution condemned attacks by Boko Haram and ISIL-affiliated groups and called for stronger regional cooperation, civilian protection, humanitarian access, accountability, and stabilization. Beyond sanctions, the Security Council Counter-Terrorism Committee, supported by its Executive Directorate, monitors states' implementation of relevant Security Council resolutions and identifies gaps and technical-assistance needs.¹⁸² Since 2017, progress has been mixed. Insecurity continues, and many communities still need protection and assistance. Resolution 2349 created a framework for cooperation, but its goals have not yet been fully achieved.

On 23 February 2020, the UNSC's ISIL and Al-Qaida Sanctions Committee added ISWAP to its sanctions list because of the faction's association with the Islamic State and its involvement in financing, planning, recruitment, arms transfers, and attacks.¹⁸³ This designation subjects ISWAP to the Security Council's ISIL and Al-Qaida sanctions regime, including an asset freeze, travel ban, and arms embargo. The regime is administered by the Security Council's sanctions committee with support from its Analytical Support and Sanctions Monitoring Team.

Nigeria has also established a national sanctions system under its 2022 terrorism legislation. This implements targeted financial measures and enforces relevant UNSC sanctions. In April 2026, the Nigeria Sanctions Committee published a list of 48 individuals and 12 entities suspected of supporting or financing terrorism.¹⁸⁴ The designated individuals reportedly included Boko Haram members, an ISWAP commander, and an ISWAP member accused of coordinating financing through cryptocurrency and online scams.¹⁸⁵ Nigerian sanctions measures have included asset freezes and travel restrictions intended to prevent designated individuals and organizations from moving or accessing funds.¹⁸⁶ Asset freezes require financial institutions,

cryptocurrency platforms, border agencies, and foreign governments to identify designated individuals and trace assets that may be hidden through informal networks or intermediaries.¹⁸⁷

Ransom payments can help criminal groups stay well-funded, even with sanctions and other measures. Nigerian law prohibits ransom payments, yet families may continue to pay when they believe the government cannot rescue their relatives.¹⁸⁸ Disrupting ransom flows without compromising the safe return of a victim is a delicate balance. Aggressive enforcement of Nigeria's anti-ransom laws may discourage families from reporting cases or cooperating with authorities.

International partners have supported Nigeria with counterterrorism training, maritime and border security, and efforts to identify terrorist financing.¹⁸⁹ These programs can improve Nigeria's ability to disrupt armed groups. UN agencies and international partners have funded humanitarian relief, reconstruction, livelihood programs, community reconciliation, and the reintegration of people leaving armed groups. The UNDP Regional Stabilization Facility has supported infrastructure, essential services, livelihoods, and the restoration of state presence in conflict-affected communities.¹⁹⁰ UNICEF, IOM, OCHA, UNHCR, the World Food Programme, and other organizations also support reintegration, displacement response, food assistance, protection, education, and humanitarian coordination.¹⁹¹ These programs reflect the view that military victories will not be sustainable unless civilians have security, services, livelihoods, and confidence in public institutions.

The international response has already included national and regional military operations, the MNJTF, targeted sanctions, financial restrictions, counterterrorism training, humanitarian assistance, stabilization projects, and deradicalization and reintegration programs. These measures have recovered territory, disrupted networks, encouraged defections, and assisted civilians, but they have not ended

the insurgency.¹⁹² The Security Council must therefore decide whether existing measures need stronger implementation or whether the changing security situation requires new approaches.

Bloc Analysis

The situation in Nigeria is complex, as the country faces overlapping security, humanitarian, social, and economical challenges. Terrorist activity remains a major threat. Additionally, broader instability is also driven by poverty, inequality, weak access to essential services, and overall regional insecurity.

These interconnected challenges create different priorities among members of the Security Council. Some states support increased military, intelligence, and counterterrorism assistance to strengthen Nigeria's ability to combat terrorist organizations. Other states place greater emphasis on humanitarian assistance, civilian protection, and accountability for human rights violations.

Lastly, some countries emphasize Nigeria's sovereignty and the principle of non-interference in domestic affairs. The central debate, therefore, relates to what form of assistance and how much influence countries should have over Nigeria's situation. Although these blocs may disagree over the appropriate balance between security, sovereignty, and human rights, all three recognize the importance of supporting regional stability and protecting civilians from continued violence.

COUNTRIES SUPPORTING COUNTERTERRORISM AND SECURITY

Terrorism and armed violence are a major security challenge in Nigeria, particularly in the northeast. Countries in this bloc would likely argue for strengthening Nigeria's security institutions, weakening Boko Haram and ISWAP, and restoring government control in affected areas. States in this bloc would emphasize the scale of the terrorist threat, supporting stronger military cooperation, intelligence sharing, regional operations, border security, and measures to disrupt extremist groups and their financing.

For instance, the United States has worked with Nigeria to combat terrorist groups through intelligence sharing, military training, equipment, and other counterterrorism efforts. In May 2026, US and Nigerian forces conducted a joint operation that allegedly killed ISIS commander Abu-Bilal al-Minuki in the Lake Chad Basin. The operation shows the current stance of the US while providing military support and working alongside Nigerian forces to address security threats.¹⁹³

Additionally, the US deployed 200 troops to Nigeria in 2026 to provide technical and training support. Similarly, France supports Nigeria's fight against terrorism. Unlike the US, France focuses on training Nigerian forces and intelligence assistance while allowing Nigeria to lead operations. France therefore emphasizes strengthening Nigeria's long-term counterterrorism capabilities rather than directly leading military operations.¹⁹⁴ While these countries may disagree over whether foreign

Additionally, the US deployed 200 troops to Nigeria in 2026 to provide technical and training support.

forces should participate directly, countries within this bloc share the same goal of reducing terrorism and strengthening Nigeria's long-term security. They might argue that humanitarian and development programs will have limited success until armed groups are weakened and affected communities are secured. They likely place immediate counterterrorism operations at the center of the international response.

HUMAN RIGHTS & CAPACITY BUILDING

Nigeria's insecurity cannot be addressed through military action alone. Countries in this group would emphasize strengthening Nigerian institutions, protecting civilians, improving access to essential services, supporting displaced populations, strengthening local institutions, investigating alleged abuses, supporting the rehabilitation and reintegration of former fighters and captives, and addressing the economic conditions that contribute to instability. They would support UN technical assistance and international funding for humanitarian programs as well as education, healthcare, livelihoods, and community-based peacebuilding.

For instance, the UK has supported and expanded cooperations with Nigeria. In March 2026, the UK allocated 746 million pounds to upgrade two Nigerian ports, ultimately using international investment to improve infrastructure, create jobs, and strengthen public services. The UK has had a focus on long-term improvement of livelihoods and addressing the conditions that contribute to instability.¹⁹⁵ Members of this bloc may still support counterterrorism assistance, but they would be more likely to condition military support on human rights training, stronger targeting procedures, detention protections, and credible investigations of alleged abuses.

Countries in this bloc argue that lasting security in Nigeria requires addressing both immediate threats and the underlying challenges that contribute to the current situation. They would support international assistance, civilian

protection, and the improvement of essential services, while allowing Nigeria to remain central to deciding how that assistance is implemented. Unlike Bloc 1, these countries would place greater emphasis on protecting civilians and addressing the conditions that enable armed groups to recruit members and control communities.

NON-INTERVENTION & SOVEREIGNTY BLOC

This bloc would emphasize that Nigeria should remain in control of its own security policy. International actors should assist Nigeria when requested, but should not impose military operations, intrusive monitoring mechanisms, externally directed investigations, or policies that undermine Nigerian sovereignty. They would favor government-requested assistance, bilateral cooperation, regional African mechanisms, and respect for the principle of non-interference. They may particularly favor cooperation through the African Union, ECOWAS, the Lake Chad Basin Commission, and the Multinational Joint Task Force.

For instance, China strongly supports Nigeria's sovereignty and has opposed foreign interference in its internal affairs. China has criticized countries like the US for the use of human rights or religious persecution claims as justification for foreign military action. While China supports international cooperation to combat terrorism, it favors cooperation requested by the Nigerian government and conducted through bilateral or multilateral frameworks, rather than externally imposed military intervention.¹⁹⁶ Russia has supported this position, calling for respect for Nigeria's sovereignty and international law while favoring diplomatic engagement rather than outside military action.¹⁹⁷

Overall, this bloc is likely to support international cooperation, but only when it is carried out with the involvement and consent of the Nigerian government. Rather than rejecting outside

assistance, these states would seek solutions that strengthen Nigeria's own security capacity while preventing external actors from determining how Nigeria manages its internal affairs. Their central concern is therefore who should control the response and under what authority.

Committee Mission

The United Nations Security Council is the primary UN body responsible for maintaining international peace and security. Unlike many UN bodies, the UNSC can adopt legally binding resolutions and authorize sanctions, peacekeeping operations, and in some circumstances, the use of force. Similarly, the Council works with regional organizations, including the AU and ECOWAS to address conflicts and security threats. These responsibilities make the situation in Nigeria particularly relevant to the UNSC as the country faces interconnected challenges involving terrorism, organized crime, regional insecurity, and weakness in governance. The Council has recognized these connections through Resolution 2349 which addressed violent extremism and the humanitarian and development challenges in the Lake Chad Basin.¹⁹⁸

The UNSC has engaged with Nigeria emphasizing the importance of peacebuilding, climate resilience, data-sharing, and cooperation between national and regional actors. The Lake Chad Basin Commission and the Multinational Joint Task Force also demonstrate the importance of regional approaches to both security and development. The Council can support Nigeria through measures such as intelligence-sharing, capacity building, regional cooperation, humanitarian assistance, and more. Delegates of the UNSC face the challenge of balancing immediate counterterrorism efforts with longer-term capacity building and respect for national sovereignty. Delegates should consider how the international community can

help the country protect civilians and strengthen its security institutions without undermining Nigerian decision-making. Solutions should address the conditions that allow insecurity to persist, including displacement, limited economic opportunities, and weak access to basic resources. The goal is to develop measures that strengthen Nigeria's ability to address terrorism and regional insecurity while promoting long-term stability.¹⁹⁹

TOPIC B

UNSC-B | NHSMUN 2027

Peace and Security in the Age of Cyber Warfare



Photo Credit: U.S. Air Force photo by Staff Sgt. Devin Boyer

Introduction

Throughout recent decades, the internet has transformed nearly every aspect of life. From civilians to governments, the world relies on digital systems to communicate, operate critical infrastructure, access information, and grow as a community. Unfortunately, as society's dependence on cyberspace grew, so did the consequences of disrupting it. Cybersecurity, once primarily concerned with protecting individual computers and private information, has been forced to evolve into a matter of international peace and security.

Since cyberspace does not conform to geographic boundaries, the threat posed by cyber operations is particularly concerning. Malicious actors can reach their target from across the world, without needing to be physically present or even nearby. In addition, the nature of cybercrime offers many opportunities for the perpetrators to conceal their identity. This makes cybercrime extremely difficult to attribute and prosecute, while simultaneously creating new opportunities for states, terrorist organizations, and criminal groups to exploit cyberspace for their own gain.

According to the Council on Foreign Relations, thirty five countries are suspected of sponsoring cyber operations over the past two decades, highlighting how cyber capabilities have become an increasingly important tool of state power.²⁰⁰ These attacks can put civilian lives at risk, heighten existing tensions between states, and cause massive financial and reputational loss for large corporations. This was the case in 2025 when cyberattacks targeting automotive supply chains in the United Kingdom resulted in an over EUR 400 million loss for Jaguar Land Rover.²⁰¹

The different forms of cyber operations only add to the complexity. No single solution can address every aspect of the issue. Cybercrime is broadly defined as any illegal activity which involves the internet, computers, or network devices.²⁰² Within this realm, there are multiple different forms of cybercrime, with varying objectives and scales of harm. Cyberterrorism involves attacks carried out by terrorist organizations to disrupt critical

systems and instill fear.²⁰³ State-sponsored cyber operations, on the other hand, are malicious cyber activities supported by a country or group of countries, often aiming to further their own interests. While the methodology used may be similar, the actors and their motivations make the difference. Finally, cyberwarfare refers to the use of cybertools during times of conflict between states.

This has presented a uniquely difficult challenge for the international community, including the Security Council. States widely disagree on the applicability of existing international law to cyberspace, such as the United Nations Charter and the Geneva Conventions. Moreover, these frameworks far predate cybercrime, and thus fail to tackle the more complex parts of the issue.

To date, there is no comprehensive system to help states agree on how international law should be interpreted, who should have authority to investigate cyberattacks, and how responsible actors should be held accountable. The Security Council must determine how to protect cyberspace without escalating the very conflicts it seeks to prevent. The central challenge is therefore not simply combating cybercrime, but establishing effective mechanisms for accountability, protecting civilian infrastructure, and maintaining international peace.

History and Description of the Issue

CYBERSECURITY AND THE DIGITAL AGE

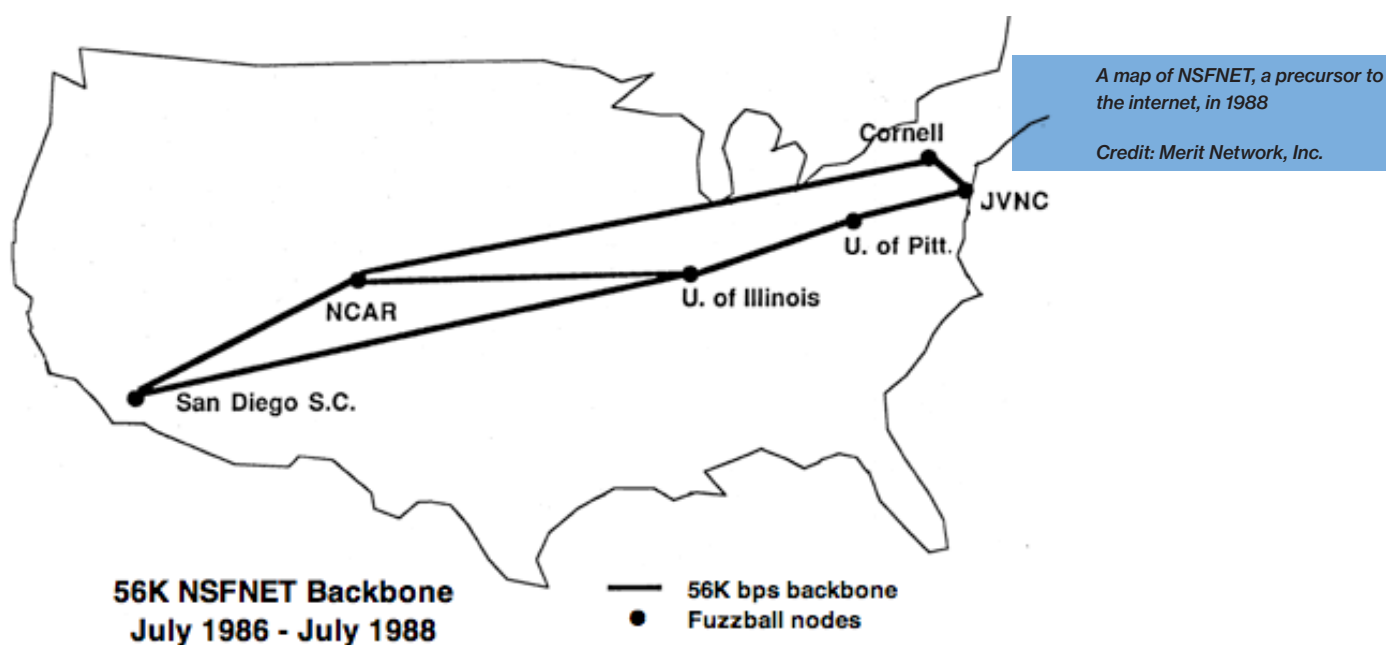
In the United States alone, federal information agencies reported over 32,000 information security incidents in 2023.²⁰⁴ Cybersecurity is the countermeasure, defined as the art of protecting data, devices, and networks from unauthorized agents and illicit users.²⁰⁵ These protections are guided by the three pillars of cybersecurity, known as the CIA triad: confidentiality of personal data and proprietary information, integrity in guaranteeing authenticity, and availability of the protected information through timely access.²⁰⁶ With the dawn of the digital age, cybersecurity has become a strategic necessity. Over the last four decades, cyberattacks have evolved from individuals targeting personal computers to a significant threat to social and economic stability.

The first internet virus, “Creeper,” was created by Bob Thomas in 1971.²⁰⁷ Notably, the idea behind Creeper was not harmful. Thomas was working on a simulation system for air traffic

control, and simply wanted to move his work from one computer to another without stopping its ongoing process.²⁰⁸ This eventually gave rise to new iterations, including “Rabbit,” the first malicious use of Creeper.²⁰⁹ While this was not as alarming at the time, society’s growing reliance on technology indicated it would soon become a bigger issue. The growing popularity of personal computers and the advent of the World Wide Web played a major role in this reliance, as computers became a common sight in average homes.

Between 1986 and 1987, the existing online network went from 2,000 hosts to 30,000.²¹⁰ By 1996, the number of existing websites had grown to 100,000, and the most popular web browser had 10 million global users.²¹¹ With this massive boom, the internet became the easiest and most cost effective way for companies, governments, and individuals to store information, reach a wider audience, and communicate over long distances, contributing towards society’s growing dependence upon technology.

This dependence was the driving force for cyberattacks becoming more organized and strategic, shifting away from individuals and towards larger entities.²¹² In 1981, the world



saw its first-ever conviction for a cybercrime after Ian Murphy, who operated under the alias “Captain Zap,” successfully hacked into multinational telecommunications company AT&T’s internal network to alter their metered billing clocks.²¹³ A few years later, the first major cyberattack, dubbed “the Morris worm,” crippled approximately ten percent of all computers connected at the time, exposing massive vulnerabilities in network infrastructures.²¹⁴ The issue eventually became concerning enough for states to address it directly. In 1986, the United States Congress passed the Computer Fraud and Abuse Act, which criminalized unauthorized computer access, with certain exceptions for good-faith security research.²¹⁵ In addition, the United Kingdom’s parliament passed the (now repealed) Data Protection Act of 1984, soon followed by the Computer Misuse Act of 1990.²¹⁶ Written for a much simpler computing era, this initial legislation would eventually fail to keep up with technological innovation.

As the general population discovered the internet’s potential for disruption, this era also gave rise to “hacktivism.” Hacktivism is a form of online activism rooted in direct action and resistance, aiming to disrupt systems without an end goal of causing harm and without personal financial motivations.²¹⁷ During times of conflict, hacktivism can present a safer, more cost-effective way for civilians to fight back against oppression. However, it carries the risk of worsening existing tensions between civilians and the state, as well as between different states depending on who is targeted.

Throughout the last few decades, hacktivism has gone from a few individuals to large, organized groups. The largest association of European hackers, known as the Chaos Computer Club (CCC), consists of approximately eight hundred hackers joined in a shared belief that information should be free, private data should be protected, and technology should improve life.²¹⁸ Presently, one of the most well-known hacktivist groups is the collective “Anonymous.”²¹⁹ Anonymous has fluid membership and no formal leadership,

emphasizing end goals of resisting censorship, promoting access to information, and supporting free speech. Among their most famous operations are their 2008 attack on the Church of Scientology, their 2009 “Operation Payback” targeting large financial companies such as PayPal and Mastercard, and their 2011 attack on private digital security firm HBGary Federal, which ultimately led to the CEO’s resignation.²²⁰

Eventually, the spread of cybercrime and hacktivism left governments and large corporations particularly vulnerable, leading to the rise in ethical hacking. Ethical hacking, unlike hacktivism, is a service typically contracted by large entities aiming to find cybersecurity weaknesses before malicious agents can do so.²²¹ Ethical hackers are cybersecurity experts trained to simulate cyberattacks, exposing vulnerabilities and allowing the target to address them before they are discovered by outside agents. The practice predates the term itself, with some of the earliest examples being the United States’ “Tiger Teams” in the 1970s. In present times, ethical hacking primarily focuses on preventing data leaks, protecting sensitive information, and avoiding financial or reputational loss. In February 2026, a group of ethical hackers from security firm Hexens successfully simulated an attack that put seventy billion USD in digital assets at risk, allowing a patch to be deployed before any losses.²²²

Having evolved alongside technology, cybercrime now presents a tangible threat to international security, heightened by society’s growing dependence on the internet. To fully understand the severity of the issue, it is important to know not only the potential consequences, but also the evolution of cyberspace and the different agents working within it.

MODERN CYBERTHREATS AND THEIR IMPACT

“Cybercrime” is a general term used to describe various offenses, each with their own

methodology and impact. Thus, before solutions can be explored, it is important to understand the depth of the issue and the different cyberthreats facing both individuals and governments. For the purposes of international peace and security, the most common objectives for cybercrime include disruption and sabotage, espionage and data theft, extortion and financial gain, and influence operations.

Malicious software, usually referred to as “malware,” is a code or program specifically written to disrupt computer programs. Malware is a broad category which includes tools used to commit cybercrime. A major component to the spread of malware and other cyberthreats is social engineering, defined as the use of psychology to manipulate people into compromising their own security. When used for cybercrime, attackers will typically pose as a trusted person, a well-known organization, or make an enticing offer to fool the victim into downloading certain files or giving out their sensitive information.²²³ One of the most famous uses of social engineering in cybercrime is phishing, a form of cyberattack involving falsified information that tricks receivers into sending assets or providing sensitive information. According to the United Kingdom’s Office for National Statistics, the most likely to be targeted are adults aged 25 to 44, a demographic that has the highest disposable income in the region.²²⁴

Disruptive operations aim to dismantle, disable, or block another state’s networks, often targeting critical systems and infrastructure. The most common, denial of service (DoS) and distributed denial of service (DDoS) attacks, function by

flooding the target’s websites and servers with excessive traffic, aiming to overwhelm them and exhaust their resources.²²⁵ Attackers use a series of bots, referred to as “botnets,” to essentially swarm the target. This can delay or otherwise disrupt service for any length of time, resulting in poor website functionality or even knocking websites entirely offline. During times of conflict, states can utilize this technology to target one another’s critical infrastructure, amplifying its destructive power.

Oftentimes, malicious cyber actors are motivated by financial gain, leading to a rise in cyber operations that aim to extort and steal from individuals or large corporations. One of the most prevalent forms of malware, known as ransomware, is the unauthorized encryption of files within a device, used to hold the device hostage until the owner pays the malicious actor to have it removed. Ransomware is not limited to affecting devices or data, but rather can be used to infect entire networks. According to the Council of Europe, ransomware can be responsible for delays, shortages, and increased product costs due to supply chain disruptions, as well as reputational loss for the targeted entity, permanent loss of valuable data, and regulatory non-compliance.²²⁶

In addition, users can be fooled into downloading a form of malware called cryptojacking, which utilizes someone else’s device to mine cryptocurrency without their consent. In some cases, attackers have used artificial intelligence (AI) to mimic another individual’s voice and appearance through techniques known as voice cloning and deepfakes, respectively.²²⁷

Attackers use a series of bots, referred to as “botnets,” to essentially swarm the target.

Attackers can then engage in “spear phishing,” which involves posing as either trusted people, or members of trusted organizations to fool their victims into sending them money, assets, and sensitive information.²²⁸ In 2024, the United States reported ten billion USD losses to scam operations utilizing voice cloning and deepfakes, stemming from massive centers in the Southeast Asia region.²²⁹

With more data being stored online, malware that can steal sensitive information has become more common. Spyware is a form of malware which gathers information from the target’s computer without their knowledge or consent. According to the United States’ Cybersecurity and Infrastructure Security Agency, spyware can capture keystrokes, screenshots, authentication credentials, personal email addresses, web form data, internet usage habits, and other personal information.²³⁰ Users are often manipulated into unknowingly downloading spyware into their own devices, typically through “Trojan horses.” Trojan horses are willingly downloaded into the target’s computer disguised as a legitimate program, often as attachments in suspicious emails or free-to-download files.²³¹ Once downloaded, they can infect the user’s computer.

Additionally, hackers often steal usernames, passwords, and other sensitive information through watering hole attacks. These are security exploits where they impersonate or compromise websites commonly visited by the group they intend to victimize.²³² One form of spyware, known as keylogging, functions by tracking which keys are pressed and sending that information. Typically, this data is then utilized for identity theft, sold to advertisers, or exploited for financial crimes. Additionally, remote access malware can exploit “backdoors” to gain access to someone else’s device, allowing the attackers to access the target’s data from anywhere in the world.²³³

While the internet and new technologies are responsible for many positive advancements, cyberspace is a tool with potential for both great good and insurmountable harm, depending on

how it is wielded. What was once envisioned as a shared, interconnected space now has the potential to start, wage, and end wars. Before countermeasures can be explored, it is imperative to understand not only the cyberthreats facing states and individuals, but also the effect they have on the global political landscape.

MALICIOUS CYBER OPERATIONS AND INTERNATIONAL CONFLICT

Cyberterrorism is defined as the use of the internet and its communication platforms to conduct terrorist attacks or further terrorist causes.²³⁴ While the methodology may be similar to that used in smaller attacks, such as when individuals are targeted through ransomware or spyware, cyberterrorism is set aside by the scale of the harm done, as well as the end goal.

Cyberterrorism is not exclusively an issue of third parties or terror groups. According to the Council on Foreign Relations, thirty five countries are suspected of sponsoring cyber operations over the past two decades.²³⁵ Out of these thirty five countries, China, Russia, Iran, and North Korea were responsible for seventy seven percent of the suspected cyber operations.²³⁶ With both countries and terror groups arming themselves with cyber tools to wage war, it is imperative to understand the full extent of the issue as well as its consequences.

Through the use of malware and supply chain exploits, cyber tools have the potential to sabotage critical infrastructure, posing a massive threat to international peace. In December 2015, thousands of homes in Ukraine lost power for approximately six hours as a result of a cyberattack on their power grid. Since then, the country has reported similar attacks to their power grid, with a notable increase following the start of the Russia-Ukraine conflict in 2022.²³⁷ Similarly, in May 2023, over a dozen Danish companies operating in the critical infrastructure sector were forced offline in an attack attributed to Russian threat actor Sandworm.²³⁸ These

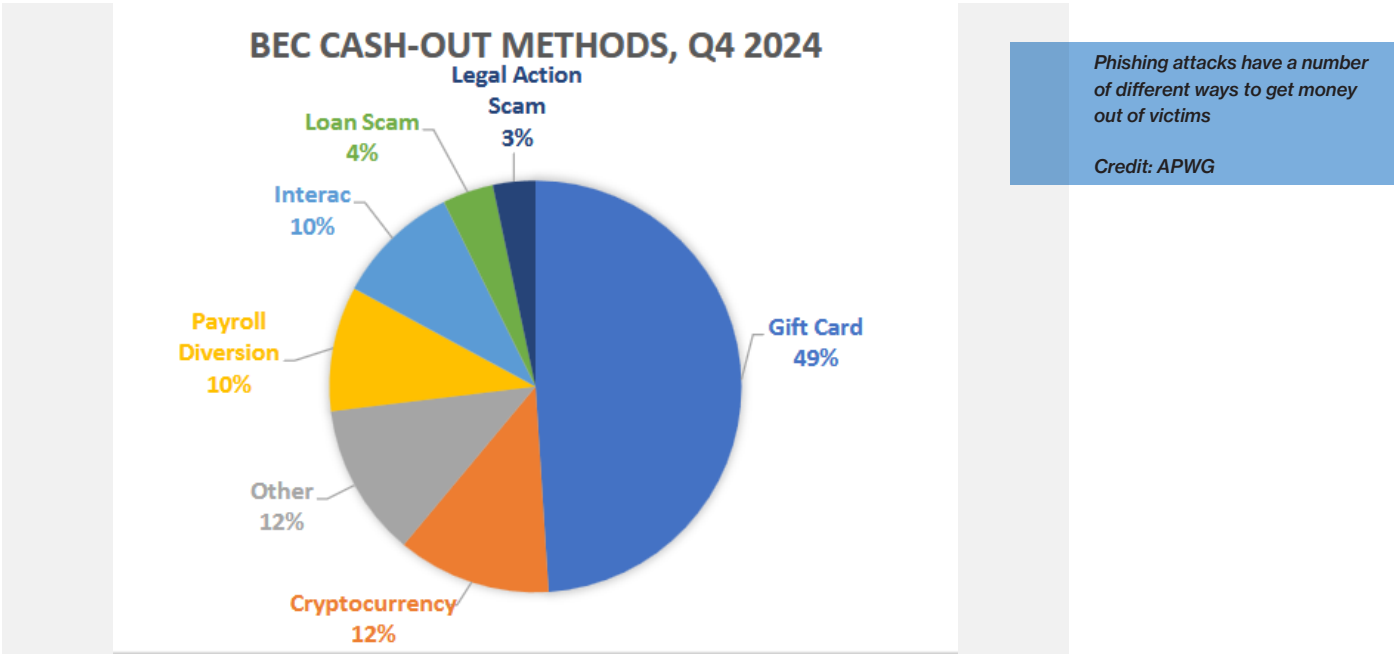
attacks have the potential to be lethal, as they target the energy, healthcare, and transportation systems. In Poland, a December 2025 cyberattack on the power grid threatened to leave half a million people without power during one of the coldest months of the year.²³⁹ This attack was later attributed to Russia, with the United Kingdom's Foreign Secretary believing it was an effort to undermine European security.²⁴⁰

In Saudi Arabia, the Shamoon virus and “Cutting Sword of Justice” breaches targeted the infrastructure used to extract natural gas and oil, destroying data from thousands of computers.²⁴¹ Targeting critical infrastructure and holding these systems hostage through ransomware allows the attacker to destabilize the target state, as countries cannot function or respond effectively to threats without proper power, healthcare, communications, and transportation systems. This successfully weakens the target state, and has devastating consequences on local civilian populations. When conducted across international borders, these disruptions can also threaten international peace and security. Attacks conducted or supported by another state, or those which cause widespread civilian harm, can lead to further hostilities or

worsen existing conflicts. Additionally, a major cyberattack may increase tensions or provoke retaliation if a targeted state believes a foreign government is responsible.

Outside this potential for sabotage, cybercrime has major strategic value for espionage. In June 2024, North Korean state-backed hacker group Kimsuky deployed malware posing as a Google Chrome extension labeled “Translatext” to steal users’ information. This operation targeted users in the United States, South Korea, and various European countries who were involved in research regarding North Korean affairs.²⁴² In September 2023, foreign embassies in Kyiv were targeted through phishing emails, shortly after the beginning of Ukraine’s counteroffensive in June 2023. According to the Council on Foreign Relations, the phishing campaign appeared to be aimed at gathering intelligence regarding foreign sentiment toward Ukraine.²⁴³

Similarly, the Chinese government is suspected of utilizing fake Signal and Telegram clones to target Uyghurs living outside of China and steal their communications data. The fake apps were uploaded to the Google Play store and are believed to have been downloaded by nearly fourteen thousand users.²⁴⁴ In February



2024, various telecommunications firms and government agencies in Israel and Turkey were targeted by Iranian group MuddyWater. This attack allowed MuddyWater to upload, extract, and monitor files directly into these systems. Sea Turtle, a group believed to be state-sponsored, was exposed in 2017 for conducting a cyber espionage operation across the United Arab Emirates.²⁴⁵

In addition, the internet allows propaganda and misinformation to spread at unprecedented rates, serving as another invaluable tool in cyberwarfare. According to the UNODC, malicious actors can use the internet to recruit civilians, radicalize them, and incite them to terrorism, as well as to plan and execute attacks.²⁴⁶ Unlike other forms of cyberwarfare, this is not a new development. The internet has been the most cost-effective way to disseminate information for decades, beating phone and fax by a wide margin, and is faster than any physical delivery without compromising the safety of the individuals gathering in one spot.²⁴⁷ By 1998, almost half of the designated terror groups on the United States' list of terrorist organizations were on the web, operating websites to incite violence and spread propaganda.²⁴⁸

In a 2002 paper, UCLA Associate Professor Vinay Lal explained "terrorist organizations [...] are increasingly resorting to the internet to disseminate their views to a wider public, and [...] have come to the realization that establishing their presence in cyberspace is nearly just as critical to their long-term success as any military triumph or act of sabotage."²⁴⁹ This use of the internet is not limited to non-state agents and terror groups, as governments have been known to disseminate propaganda through various online forums. This has given rise to "memetic warfare," where governments hijack internet culture to bypass internet users' critical thinking and skew public opinion. According to *Psychology Today*, countries such as Iran and the United States have begun heavily leaning into memetic warfare to reinforce social identity, propagate the "us-vs-them" mentality, and

normalize violent strikes against "enemies."²⁵⁰

In addition, states and third parties can use the internet to promote their preferred ideology during times of conflict. In *Networks and Netwars*, Dorothy Denning points out that NATO targeted Serb media outlets throughout the conflict over Kosovo, but purposefully ignored service providers and satellite links which kept then-Yugoslavia online, believing "full and open access to the internet" would turn the people against the Milošević regime.²⁵¹ In present times, this manifests itself through election interference and terrorist recruitment, making it a significant potential threat to global security. Cybersecurity does not extend only to the theft of information; it also includes the use of the internet to spread disinformation.²⁵²

Cyberterrorism has the potential for both short-term and long-term impact. The financial ramifications present an entirely new challenge, as certain actors use cybercrime to fund illicit operations. According to the United Nations' Multilateral Sanctions Monitoring Team (MSMT), North Korea has built a cyber ecosystem that generates hundreds of millions in revenue, successfully avoiding UN Security Council sanctions.²⁵³ This revenue, generated through malicious cyber activities including cryptocurrency theft, is then used to fund their nuclear weapons and ballistic missile programs. Moreover, cyberattacks targeting election systems and campaigns can manipulate the outcomes of foreign elections and erode public trust in the existing systems.²⁵⁴ Addressing cyberterrorism presents a uniquely multifaceted challenge, requiring a similarly thorough solution.

GLOBAL RESPONSE

Cyberspace is not owned, controlled, or managed by any specific state or entity. Instead, it is a shared, decentralized space built by millions of willingly interconnected networks. While this may imply no government is responsible for securing cyberspace, the opposite is true.

Every government has a responsibility, not only to their own population but to all, to ensure their agents use the internet responsibly and without malice. Article 2(4) of the United Nations Charter explicitly prohibits the threat or use of force against another state's integrity or independence.²⁵⁵ Whether cyberattacks violate Article 2 is largely dependent on their effect.

The emerging consensus indicates that cyberattacks resulting in damage to property, injury to a person, or loss of life are in violation of Article 2's prohibition on the use of force.²⁵⁶ Additionally, there are growing concerns over whether cyberattacks which fail to meet this threshold can still be considered as violations of Article 2(4), on account of their potentially detrimental effects on national security.

The United Nations has historically recognized the threat posed by cybercrimes. The UN General Assembly Resolution 55/63, "Combating the Criminal Misuse of Information Technologies," was a non-binding document that laid vital groundwork for future discussions regarding cybersecurity and the digital age. Passed on 22 January 2001, it focused on the measures states could take to eliminate cyber offenses within their borders, such as developing their information systems with heightened security in mind, prioritizing international cooperation in the prosecution of cybercriminals, and allocating resources to training law enforcement agencies on cyber issues.²⁵⁷

In addition, the Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, entered into force on 1 July 2004. Considered the first international attempt at addressing cybercrime, it aimed to combat the "borderless" nature of cyberspace by aligning national laws, as well as encouraging states to work together in their investigation and potential prosecution of cyberthreats.²⁵⁸ Presently, the convention has 82 participating parties and 15 signatories.²⁵⁹

More recently, the UN Global Mechanism

on ICT Security was established to promote responsible state behavior within cyberspace.²⁶⁰ This permanent forum was established in 2026, but it builds upon the foundation laid out by the 2021–2025 Open-Ended Working Group.²⁶¹ The Global Mechanism is an example of new legislation aiming to hold states accountable for their behavior in cyberspace, recognizing that international law applies to these spaces as well. These resolutions and forums are vital steps towards addressing the dangers posed by cybercrime, emphasizing international cooperation and open communication between different response teams.

More recently, the United Nations Convention Against Cybercrime was adopted by the General Assembly on 24 December 2024. The first fully global treaty addressing cybercrime, it aims to strengthen international cooperation and provides a range of measures states can take to prevent and combat cyberattacks.²⁶² The Convention's nine chapters call for a variety of measures states must take while combating cybercrime, such as adhering to their obligations under international and human rights law, criminalizing the most prevalent forms of cybercrime to overcome the perception of impunity, making cybercrime inherently international to ensure criminals cannot exploit jurisdictional gaps, and for states to share their findings with one another regarding cybercrime trends and methods so the international community can build a safer world together. The Convention has not been ratified as of August 2026, but the United Nations is urging states to ratify, implement, and support it, particularly in developing countries.²⁶³

Furthermore, the United Nations Office of Counter-Terrorism adopted the Global Counter Terrorism Programme on Cybersecurity and New Technologies in April 2020.²⁶⁴ This Programme provided capacity-building support to the United Nations' member states, aiming to develop and implement more effective responses to the threats posed by the internet. More specifically, the Programme plans to meet this objective

Signing ceremony for the United Nations Convention Against Cybercrime in Viet Nam

Credit: VNA



through enhancing the skills and capabilities of these countries and their citizens when it comes to effective anti-terrorism policy, protecting critical infrastructure from cyberattacks, and enhancing criminal justice capabilities to counter and investigate the malicious use of new technologies. This is made possible through the funding provided by the European Union, Germany, Japan, the Republic of Korea, Saudi Arabia, and the United Arab Emirates.

As cyberterrorism and its consequences advance, private agencies and large corporations have become more involved in tackling the issue, seeing themselves as likely to be targeted as state governments. On 17 December 2025, tech giants such as Meta and TikTok met with representatives from sixty seven countries in Bangkok, Thailand to launch the Global Partnership Against Online Scams, an international coalition aiming to dismantle transnational cyberfraud networks.²⁶⁵ While online scams may not always pose a direct threat to international security, the income from these scams often does, as malicious actors use them to fund their operations.

As such, this partnership is committed to ensuring cybercriminals face justice through effective investigation and prosecution, and to further public-private partnerships to ensure governments can keep up with cyber advancements.²⁶⁶ If successful, this would deprive international crime groups from the funding obtained through online scamming, furthering global peace and stability. Moreover, this is a significant step towards getting private corporations to support the fight against cyberterrorism and fraud.

Tech giants often have the resources and expertise that rival those of smaller, developing states. Involving them in the fight against cyber scams can help overcome the financial barriers which have left some states more vulnerable than others, and is a strong step towards amicably regulating new technologies and their use. To preserve international peace, the Security Council can potentially rely on these private companies to preserve evidence, share information regarding threats they face, block sanctioned actors, and assist states in effectively responding to cyberattacks.

Along with drafting new regulations, it is also vital to consider how cyberspace interacts with rules and laws drafted before its existence. The Geneva Conventions, adopted on August 12, 1949, are a set of four treaties governing the treatment of wounded and sick armed forces, prisoners of war, and civilians during armed conflict. The Fourth Geneva Convention focuses specifically on the protection of civilians.²⁶⁷ While some have called for the creation of a “Digital Geneva Convention,” the current Geneva Conventions and Additional Protocols are already part of international law.²⁶⁸

International humanitarian law, therefore, applies to cyber operations conducted during and sufficiently connected to an armed conflict, but not to ordinary cybercrime or every hostile cyber operation conducted during peacetime. During an armed conflict, cyber operations must follow rules protecting civilians, including the principles of distinction, proportionality, and precaution. It is helpful to consider whether existing international treaties can and should apply to new technologies; international law needs to keep up with scientific and technologic advancements, but it is possible for documents such as the UN Charter and the Geneva Conventions to be applicable even if they predate the issues. While passing new legislation is helpful, it is also vital to consider where existing legislation has fallen short, and where it has simply failed to be enforced when appropriate.

Current Status

ADVANCEMENTS IN MALICIOUS CYBEROPERATIONS

Governments have begun treating cyberspace as another arena for global power. To this end, state-sponsored cyberattacks are malicious cyber operations that are supported by a country or group of countries, rather than by unaffiliated individuals or third parties.²⁶⁹ With geopolitical

tension and international conflict on the rise, state-sponsored cyber activity has become exceedingly alarming. Countries have realized the destructive potential and cost-effectiveness of cybercrime, particularly as more industries go digital and more governments become fully reliant on the internet for their basic operations. In addition, the difficulty in attributing and prosecuting cyberattacks further incentivizes their use in modern day warfare. According to Matt Shelton, Google Cloud’s head of Threat Research and Analysis, states who were once apprehensive of electronic warfare now regard cyberwar as “just another tool in their box, which they can use against their adversaries in support of national security and diplomatic aspirations.”²⁷⁰

In recent years, AI has emerged as a powerhouse in cyberwarfare innovation. Between September 2023 and February 2024, AI-powered misinformation campaigns influenced nearly 50 percent of global elections, including those in Taiwan and Moldova.²⁷¹ These campaigns utilized deepfakes and bot networks to manipulate public opinion, putting democracy at risk and calling into question the validity of the electoral process. In a similar vein, AI has revolutionized scamming. Where scams were once mistake-ridden emails and suspicious phone calls, AI has allowed scamming centers to mass produce convincing websites, emails, texts, and even imitate the voice and appearance of the target’s trusted ones.²⁷²

As the technology evolves, deepfakes and voice clones have made scams almost indistinguishable from real communications. Moreover, with AI doing the heavy lifting, scammers are able to work faster than ever and with incredible accuracy. Additionally, the barrier of entry for scamming has been substantially lowered by AI. Scammers no longer need to write convincing emails, match the tone of the individual or organization they are impersonating, or even speak their target’s language. For countries and organizations that use the income from scamming to fund illicit operations, this usage of AI presents a metaphorical goldmine. As such, AI has the potential to pose a major

threat to international peace and cooperation. AI can expand the reach and capabilities of malicious actors across the board, worsening the impacts of their operations. When AI is used to support foreign interference, conflict escalation, terrorist objectives, or to fund illicit operations, it becomes a credible threat to global security to be addressed by the Security Council.

During recent military conflicts, AI-powered facial recognition has been utilized to guide automated drone strikes, leading to a broad discussion regarding accountability and accuracy. The Israel Defense Forces (IDF) has been at the forefront of this criticism, as they continue to rely on AI-powered autonomous drones. The process guiding these drones is known as a kill chain, “a system of execution that extends from large-scale data surveillance, geolocation, and the identification of targets to their algorithmically mediated elimination.”²⁷³ The facial recognition data is gathered through a program called Lavender, developed by the IDF’s elite intelligence division.²⁷⁴ Lavender’s database reportedly houses information on over two million residents of Gaza, including age, gender, movement patterns, and social media activity.²⁷⁵ This serves as an example of how

digital surveillance and cyberintelligence can be used to support military targeting, raising concerns regarding the technology’s impact on international peace and the incentive for hackers and malicious actors to access it.

Moreover, recent years have seen a consistent rise in the use of ransomware to target sensitive data, particularly impacting the healthcare industry. Since 2015, there has been a 300 percent increase in ransomware attacks targeting hospitals.²⁷⁶ In 2024, ten percent of reported ransomware attacks targeted the healthcare industry, threatening to leak sensitive and privileged information if their demands were not met.²⁷⁷ These attacks do not target individual hospitals, but also entire networks.

On 3 June 2024, the United Kingdom’s premier pathology service provider, Synnovis, fell victim to a massive ransomware attack which resulted in severely diminished test-processing capabilities.²⁷⁸ The consequences can be absolutely devastating, making these attacks more than just white collar crimes. Studies of two centers under attack showed a significant increase in patient volume, waiting times, and patients being forced to leave without seeing a medical provider.²⁷⁹

Maia Sandu, left, won re-election in 2025 as a generally anti-Russia candidate. The campaign after a campaign marked by extensive AI-generated misinformation, widely presumed to come from Russia

Credit: Office of the President of Ukraine



This is not without consequence; in 2024, the first ransomware death lawsuit was settled after a baby born during a ransomware attack passed away at the hospital.²⁸⁰ As the lawsuit alleges, the attack rendered the hospital unable to provide proper care for the baby, who was born with health complications. Evidently, the use of cyber tools to exploit vulnerabilities in the healthcare industry is a dangerous issue requiring immediate attention. Hackers know the stakes are extremely high for hospitals; they not only handle sensitive data, but they actively work in life-or-death circumstances. This incentivizes malicious agents to target hospitals, knowing they cannot spare the time needed to address the malware and will instead likely pay the ransom. If this worrying trend continues to go unaddressed, the consequences will likely be fatal. When these attacks are state-sponsored, they pose a massive danger to global peace, as states become likely to retaliate against one another. Ultimately, the harm is not contained to the civilians in the targeted hospital, as this potential for escalation threatens the international community at large.

ATTACKS ON CIVILIAN INFRASTRUCTURE

Regardless of what a malicious actor's ultimate goal is, it is more often than not civilians who pay the price. In May 2026, thousands of students were left without access to their university's online resources after Instructure, the parent company responsible for Canvas, fell victim to a massive ransomware attack. This attack came during the busiest time of the semester, when most students are preparing for final exams and assignments. However, the damage goes further than mere academic consequences. According to the National Cybersecurity Alliance, hackers downloaded personal student data from the platform while it was offline, including names, email addresses, student identification numbers, and private messages sent through Canvas.²⁸¹

While Instructure claims to have received confirmation that the stolen data was deleted

following payment of the ransom, there is unfortunately no way to guarantee whether this is the case. The group responsible, who call themselves ShinyHunters, were able to breach the platform by sending malicious code to the support representatives. Although targeting an educational platform does not automatically threaten international peace and security, it demonstrates how a single breach can disrupt services and expose data across many institutions and locations. Similar methods become especially relevant to the Security Council when they target critical infrastructure, cross national borders, cause widespread civilian harm, or involve state-supported actors.

Historically, hackers have targeted power grids, water systems, and the healthcare sector. In April 2026, various United States intelligence agencies warned of cyberattacks by the Iranian government targeting critical infrastructure.²⁸² These warnings came after United States President Donald Trump threatened Iran's bridges and power plants. In the notice, the Environmental Protection Agency highlighted concerns that the Iranian government had "already disrupted commonly used operational technology at drinking water and wastewater systems."²⁸³ This type of attack can have catastrophic effects on health outcomes.

Access to safe, clean drinking water is essential for the survival and wellbeing of civilian populations, and the disruption of wastewater systems can contaminate food and water resources, rendering them useless. Countries with water scarcity are particularly vulnerable, as they may rely more heavily on infrastructure such as desalination plants. In Kuwait, for instance, military strikes on desalination plants threatened the water supply that ninety percent of the country relies on.²⁸⁴ Although this was a physical attack rather than a cyberattack, it demonstrates the potential consequences of disabling water infrastructure. A successful cyber operation against the same systems could similarly interrupt access to water without requiring a conventional military strike.

The energy grid is another particularly vulnerable sector with potentially catastrophic consequences. Cyberattacks on electric and gas companies can disrupt other critical processes, such as healthcare and communications, essentially bringing a country's usual operations to a halt. Energy grids are especially vulnerable due to three key reasons: a broad attack surface from decentralized locations, a strong incentive for malicious actors to extort ransom given the grid's importance, and gaps between information technology networks and operating infrastructure.²⁸⁵ This can result in power outages, supply chain disruptions, and financial and health system failures.²⁸⁶

In December 2025, Polish heat and power plants were targeted in a particularly destructive attack which threatened to leave residents without heat or power during one of the coldest months of the year. According to CERT Polska, the attacker accessed a perimeter device in a wind farm, established a VPN connection, and was then able to access the wind farm's web administration interface.²⁸⁷ The hacker utilized this access to shut down the steam turbine and water treatment systems which allow the plant to operate normally, successfully shutting down a power plant meant to provide heat for fifty thousand residents. This attack went undiscovered for months, as the Polish government was focused on a different attack on its power grid, which threatened to leave five hundred thousand people without power.²⁸⁸

Attacks on the healthcare sector can also put civilians in precarious situations, additionally threatening their privacy if sensitive medical

data is lost to a breach. In August 2026, a ransomware attack on one of Canada's largest healthcare facilities disrupted critical facility-management systems, such as doors, elevators, heating, ventilation, and air conditioning.²⁸⁹ This is a particularly concerning extortion strategy. Historically, hackers have used files, data, and information as their digital hostages. The move towards using medical infrastructure and, by extension, patients' lives to extort ransom shows a worrying trend, particularly as this form of cybercrime becomes more common.

Cyber operations targeting the transportation sector have the potential to upend the entire country's processes, making this sector a particularly enticing target. The transportation industry is not solely responsible for the day-to-day commutes of individuals, but also the movement of goods and services throughout the entire country. Moreover, the entire transportation industry is vulnerable, be it maritime, aviation, rail, or even roads. In recent years, various countries have seen cyberattacks on their transportation grid, including the United Kingdom's Network Rail, Japan's Port of Nagoya, Estonia's Elron, and the global system JAS Worldwide.²⁹⁰ The impact heavily depends on the type of incident reported.

In the Baltic region, GPS disruptions tied to Russian agents were responsible for flight diversions and suspensions, mostly impacting civilians, while in Lebanon, flight information screens at Beirut International Airport were hacked to display politically motivated messages, causing fear and anxiety for passengers.²⁹¹ Alternatively, when DP World Australia was breached, the three-day suspension of

In August 2026, a ransomware attack on one of Canada's largest healthcare facilities disrupted critical facility-management systems.

operations affected multiple shipping container terminals, resulting in a backlog of thirty thousand containers.²⁹² This has the potential to cause severe supply chain delays, as well as serious financial loss.

When civilian infrastructure is targeted, thousands of innocent lives are put at risk. The Universal Declaration of Human Rights entitles all human beings to dignity, education, and a standard of living that supports health and wellbeing, “including food, [...] housing and medical care and necessary social services.”²⁹³ In addition, the Geneva Convention provides protections to civilian hospitals, demanding they not be attacked during times of conflict.²⁹⁴ To promote global peace and security, it is vital to ensure civilian infrastructure is not viewed and treated as simply another arena through which to wage war, particularly through the use of cyber tools.

CHALLENGES IN PROMOTING CYBERSECURITY

Despite the major global response, cyberterrorism has not yet been eradicated. This can be attributed to more than one cause: inability to keep up with technological advancements and their use, disparities in the resources states have at their disposal to handle cyber threats, and difficulty in attributing cybercrimes to a particular actor, to name a few. While there may never be an all-encompassing solution that fully tackles the issue, it is possible to reduce its effects and ensure governments are better protected. To this end, it is imperative to understand where solutions and legislation have fallen short.

A major roadblock to combating cyber terrorism is the lack of a global consensus regarding who has jurisdiction over cyberspace, as well as disagreements over issues related to data collection, sovereignty over national networks, and the role private companies should play. When states disagree on who can govern the internet,

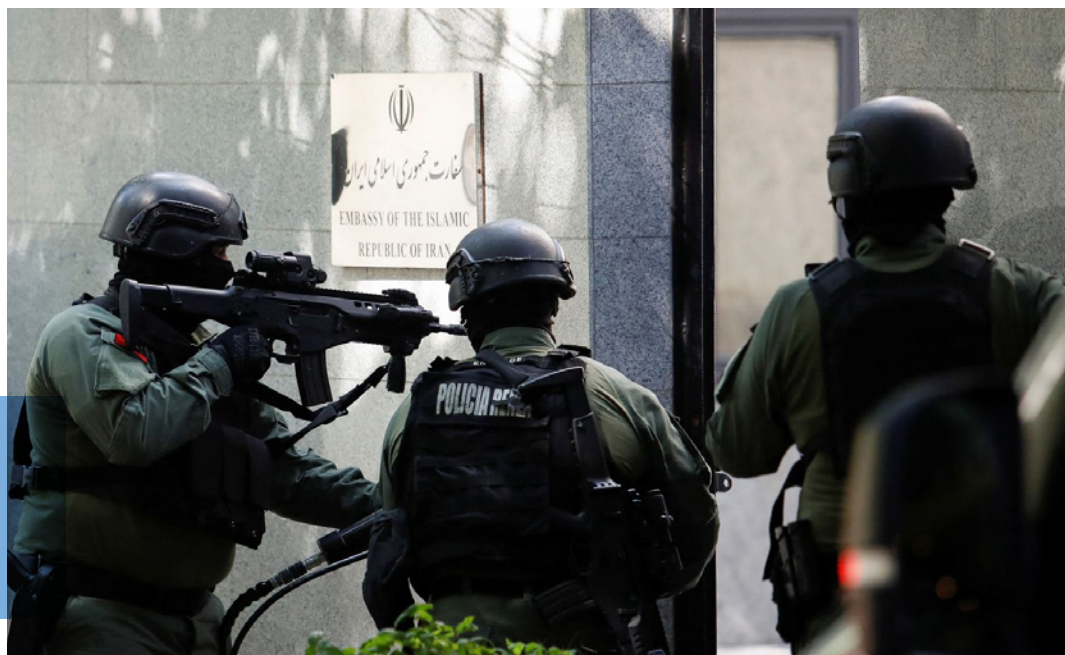
it becomes nearly impossible to attribute and prosecute cybercrimes, creating a feeling that hackers can act without consequences. Russia and China have both refused to join the Budapest Convention, citing concerns over their national sovereignty being violated if they do so.²⁹⁵ Their opposition does not necessarily mean that they reject international law in cyberspace, but rather they have objected to cross-border investigations conducted without an affected state’s consent.²⁹⁶

Instead, these states, along with Belarus, Syria, Venezuela, and Iran sponsored a resolution to adopt a new international cybercrime convention in 2019.²⁹⁷ The resolution, despite ultimately passing, received little support from the majority of Western states present. This example highlights the issue which has dominated the international conversation regarding combating cybercrime: certain countries are hesitant to support what they view as foreign intervention and an affront to their sovereignty. This is why international cooperation is vital. Countries who have hesitated to join previous treaties and treated existing regulations as inapplicable to cyberspace are unlikely to cooperate if they are not able to negotiate the terms and have full transparency regarding how new policies and regulations would impact them.

Even if the matter of jurisdiction was solved, the lack of a universal definition regarding cybercrime will pose another issue. According to the United States Government Accountability Office, different law enforcement administrations within the country – such as the Federal Bureau of Investigation, Drug Enforcement Administration, and the Secret Service – have different definitions of what constitutes a cybercrime, meaning agencies struggle to share information and coordinate their efforts.²⁹⁸ This becomes even more impactful at the global scale. If states follow their own definition of cybercrime, many offenses could be left unpunished, depending on who has jurisdiction over the offender, and countries may be unable to coordinate extradition and prosecution when relevant if they cannot agree on whether a crime

Albanian counterterrorism police enter the Iranian embassy following Albania's allegation that Iran coordinated devastating cyberattacks against Albanian government systems.

Credit: Sky News



was committed.

Additionally, the difficulty in attributing cyber offenses to particular states, groups, or actors makes it extremely difficult to prosecute them, even if all countries were to agree on a single legal framework to be followed. Attribution is widely considered one of the most complex and difficult areas of this issue, worsened by states' refusal to admit blame. Within this framework, there is technical attribution, which identifies how an attack occurred and who was responsible for it, and political responsibility, which identifies who should be held responsible for it.

Currently, the process of technical attribution involves analyzing the malware utilized, as well as routines which tie the incident to a particular known malicious actor.²⁹⁹ Moreover, the political objectives and interests furthered by the attack act as another major clue towards who could be behind it. According to the United Nations Office on Drugs and Crime, this process is known as backtracking or traceback, and it works by examining the log files (files automatically generated by systems to record any activity) and using those as an audit trail.³⁰⁰ Unfortunately,

these methods are not foolproof, and there is little to no guarantee about their accuracy.

Malicious actors keep finding new ways to disguise their identity, and it is possible for large-scale operations to remain undiscovered for months.³⁰¹ Any ideal solution to the threat posed by cybercriminals should take into account the difficulties in correctly attributing cyber offenses, as well as the international reputational harm that falsely-attributed attacks can have on member states. A state that is falsely accused will likely become uncooperative, and a state which is rightly accused will likely deny its involvement. When facing this situation, proper investigative methods and accountability mechanisms, along with a global legal framework for prosecuting serious cyber offenses, are paramount.

Cybercrime often goes underreported, adding on to the burden of reducing it effectively. Many individuals do not report cybercrime because they are simply not aware of where to do so or which agency would be most appropriate to handle it. For businesses, many hesitate to report being victimized by cybercrime, as they fear it will negatively impact their reputation

and trustworthiness.³⁰² While there have been multiple efforts to educate the public on how they can protect themselves from cyberthreats, the matter of where and how to report being victimized has not been given equal attention. Individuals and small businesses may not be the primary targets of cyberterrorists, as they are more likely to pursue critical infrastructure and military information, but the tactics used on one may be used on the other. As such, it is helpful to have information regarding as many cyber offenses as possible, which cannot occur without proper reporting and documentation.

The speed of technological advancements poses another hurdle, with some states and law enforcement agencies struggling to keep up. In recent years, supply chain attacks have become extremely relevant, accounting for approximately forty percent of cyberthreats in 2025.³⁰³ Accordingly, sixty percent of C-suite executives have pointed out supply chain attacks as their number one threat.³⁰⁴ While this format of cyberthreat is not necessarily new, the speed at which its scale, frequency, and sophistication have developed makes it difficult for companies to protect themselves and for states to investigate properly. Moreover, the implementation of new technologies such as AI has only added further complexities. With the world becoming digitized and third-party apps becoming more common, previously minor issues such as supply chain attacks quickly went from a relatively rare occurrence to the new normal. This highlights why it is so difficult to keep up with trends in cybercrime; due to changing trends and innovations, what was once seen as

a minor inconvenience not worth addressing can eventually become a large-scale issue threatening financial stability.

Bloc Analysis

When tackling cyberthreats, the Security Council's member states differ not only on their technological capabilities, but also on how international law should apply to malicious cyber operations and how responsible actors should be identified and held accountable. Some states support applying existing international law and publicly attributing attacks when national investigations identify a responsible actor. Other states argue that attribution should require an impartial international investigation and stronger public evidence, especially before the Security Council acts. They warn that unilateral accusations may be politically motivated, based on intelligence that other countries cannot independently evaluate, or used to justify interference in another state's affairs.

Some countries believe in metaphorical open borders when it comes to the internet, governed by shared international rules. Others are significantly more wary of international influence over their networks and emphasize each state's authority to control its own networks, information, and data. In the latter category, some states have enacted measures such as firewalls to isolate their civilians and protect their data, particularly when foreign access or influence could threaten national security. Some countries have already indicated, through policy or through action, a

Sixty percent of C-suite executives have pointed out supply chain attacks as their number one threat.

belief that cyberspace should be dominated by international rules and regulations. The further debate is how the international law should be interpreted, who may credibly attribute an attack, what evidence should be required, and when sanctions or other consequences are appropriate. Other states, favoring country sovereignty and non-intervention, have espoused a belief that each state reserves the right to rule over cyberspace as they do with their own land.

Through this division, the five permanent members of the Security Council, along with the ten temporary members, will naturally split into three blocs. The first bloc will include countries who support applying existing international law, publicly attributing serious attacks, and imposing consequences when sufficient evidence identifies a responsible actor. On the other hand, the second bloc will include those countries who prioritize state sovereignty, oppose accusations made by individual countries, and prefer investigations or rules agreed upon by multiple states. Finally, the third bloc may include states which share some elements of Bloc 1 and 2's positions. However, they may still be developing technologically and thus place greater immediate emphasis on capacity-building, secure infrastructure, and equal participation in international cyber decision-making.

Delegates should research their country's stance on the issue thoroughly. Country policy can be complex, with states often agreeing on particular areas but disagreeing on others. Thus, delegates are encouraged to consider whether their country supports national or international investigations, prefers existing or new global rules, supports sanctions for serious cyber attacks, and favors either an open internet or greater national control over digital systems.

EXISTING-LAW AND ACCOUNTABILITY ADVOCATES

This bloc would include the more technologically-advanced countries who believe that the United

Nations Charter and other existing international laws apply to conduct in cyberspace. These states tend to support the idea that the internet should be an open and interconnected space, rather than restricted by metaphorical closed borders. This position supports shared international rules for cyberspace; while each state and its citizens remain sovereign, their harmful actions in the shared cyberspace are subject to international laws and regulations.

Despite supporting an open internet, this bloc can still house countries with strict data laws that aim to protect their citizens from both malicious actors and corporations seeking to exploit their information. For instance, the European Union has a variety of data protection laws, such as the General Data Protection Regulation, which grants users rights over their personal information, protects private data, and is applicable to any group handling European data regardless of where in the world they are located.³⁰⁵ Furthermore, members of this bloc would seek accountability for serious cyber operations, and have historically publicly attributed some attacks to particular states based on national or coordinated investigations. They may support targeted sanctions, diplomatic consequences, and assistance to affected countries when they believe sufficient evidence identifies a responsible actor. However, critics argue that these states do not always release enough evidence for other countries to independently evaluate their accusations.

Since they are very reliant on cyberspace for their critical operations, these countries would support propositions that aim to protect infrastructure and be open to applying existing international law to cyberspace. This bloc will include countries such as the United States and the United Kingdom, as well as countries within the European Union such as Denmark and France.

SOVEREIGNTY AND INTERNATIONAL- INVESTIGATION ADVOCATES

States within this bloc would generally be as technologically-advanced as the first bloc, but place greater importance on national sovereignty, state control over digital systems, and protection from foreign interference. These countries do not necessarily reject the application of international law to cyberspace. Instead, they may disagree about how existing rules should be interpreted, whether new agreements are needed, and who should determine that a violation occurred.

Countries in the second bloc would weigh the security threats posed by an open internet, and be wary of foreign interference, losing the right to regulate their citizens' content and data, and following international rules that would conflict with their domestic policies. These countries have historically placed great importance on non-interference, believing they have a right to rule over their constituents even within cyberspace. In this view, the internet is not a separate, shared space, but rather an extension of national sovereignty. This gives states the right to control their own information spaces and regulate their digital infrastructure.

For example, the Chinese government has famously relied on a system of laws and computer tools to restrict their citizens' access to foreign media and websites, colloquially dubbed the "Great Firewall."³⁰⁶ The Chinese government describes these controls as necessary to protect national security, public order, and its domestic information environment. Critics argue that the same system limits political expression and access to information critical of the government.

Delegates should consider the full extent of these policies and how their countries may both benefit and suffer from their proposals. Moreover, since countries within this bloc may disagree with how existing international rules are interpreted, they are likely to support new agreements negotiated through the United Nations. Unlike the first bloc, members of this bloc oppose

accusations made by individual countries and prefer investigations agreed upon by multiple states. They may also demand stronger public evidence before the Security Council imposes sanctions or other consequences. This bloc will include countries such as Russia and China.

CAPACITY-BUILDING AND CYBER- RESILIENCE ADVOCATES

Finally, the third bloc would welcome those states whose cyber capabilities are still growing. For many developing states, their key focus is not on whether an open internet represents a challenge to country sovereignty, but rather how they can participate in cyberspace without becoming more vulnerable to cybercrime and foreign interference. However, these states may still align with either of the first two blocs on international law, attribution, sanctions, and national control over information.

The UN has recognized that developing countries are at a higher risk of being targeted by cyberattacks, and that they would face a disproportionately high economic impact if their critical infrastructure, banking systems, and healthcare sector were to be attacked.³⁰⁷ As such, these countries would most likely prioritize building secure digital infrastructure and strengthening international coalitions to support their existing systems. This would make states within this third bloc more likely to support cybersecurity capacity-building programs, the international sharing of expertise and cybersecurity trends, and global mechanisms for reporting and responding to cyberthreats.

Countries within this bloc would aim to protect critical infrastructure from cyberattacks and favor solutions that incorporate technology in more financially accessible ways. They may support international funding, regional cybersecurity centers, and training programs. At the same time, they may oppose assistance that gives foreign governments or companies access to sensitive data or creates long-term dependence on

outside technology. It is also vital to consider that not all countries within this bloc would fully favor an open internet, as some will likely be wary of foreign interference, espionage, and the cultural impact of globalization.

These countries may therefore favor assistance that is voluntary, affordable, transparent, and adapted to national needs. They are also likely to demand a meaningful role in creating international cyberwarfare rules rather than accepting standards developed mainly by technologically powerful countries. This bloc will include countries such as Somalia, the Democratic Republic of the Congo, and Liberia.

Committee Mission

The United Nations Security Council is one of six main organs established through the United Nations Charter. Tasked with maintaining international peace and security, this committee is unique in its ability to enact economic sanctions and arms embargoes, sever diplomatic relations, and call for collective military action.³⁰⁸ In addition, Chapter VII of the United Nations Charter allows the Security Council to completely or partially interrupt economic relations as well as “rail, sea, air, postal, telegraphic, radio, and other means of communication.”³⁰⁹ As a United Nations body, the Security Council shares in the principles of diplomacy and compromise which guide the organization as a whole. Thus, before resorting to the measures outlined above, member states are encouraged to call upon any offending parties to comply and attempt to reach a peaceful compromise.³¹⁰

As mandated, the Security Council discusses the most pressing issues threatening international security, focusing on preventing future crises and lessening the present ones. While the Council has previously discussed issues relating to cybersecurity, it has never created a comprehensive system governing state conduct within cyberspace, making this an imperative

in the digital age. Historically, sanctions and punitive measures have heightened tensions and furthered division in already-violent conflicts. This all but negates the possibility of a peaceful resolution, making it vital for delegates to engage in good faith and think critically about potential solutions and their consequences. While the Security Council can enact sanctions and order intervention, delegates should consider all alternatives before landing on the most invasive solutions. The Security Council's mandate compels this body to protect international peace above all; a solution which will simply generate more conflict down the road will fall short of this goal.

When drafting resolutions, delegates should consider the applicability of existing legislation to cyberspace, including the UN Charter. This will serve as a primary point of division, as states have historically disagreed on whether cyberspace can be governed in this way, particularly where existing legislation was drafted long before the digital age and does not explicitly take cyberthreats into account. Moreover, delegates should be aware of the primary issue in prosecuting cybercrime: the difficulty in attributing them to a specific state or entity. Unlike physical attacks, which require some level of presence, cybercrime can target anyone across the globe, and states will seldom admit to their role in any form of state-sponsored violence. Delegates must consider how the Security Council can investigate serious cyber operations, protect civilian infrastructure, assist affected states, and hold responsible actors accountable without responding to uncertain evidence or escalating international tensions.

Finally, delegates should consider the full extent of this technology and its uses. While it does pose a threat to international peace, cyberspace can be used for good and even be part of the solution. The internet has the potential to connect civilians across the globe, serving as a bastion for mutual aid during times of conflict and informing the international community. Additionally, hacktivism can put pressure on

governments and corporations. While cybercrime is a real threat, the technology upon which it relies can revolutionize healthcare, predict economic trends, connect people, and overall improve society. The solution is not to villainize or ban the technology itself, but rather its misuse.

Research and Preparation Questions

Your dais has prepared the following research and preparation questions as a means of providing guidance for your research process. These questions should be carefully considered, as they embody some of the main critical thought and learning objectives surrounding your topic.

TOPIC A

- 1 How should the Security Council help Nigeria combat Boko Haram and ISWAP while limiting civilian harm and protecting human rights?
- 2 How can Nigeria, neighboring states, and international partners restore regional military cooperation and intelligence sharing in the Lake Chad Basin?
- 3 Should international support focus mainly on military operations, or should it give greater attention to governance, poverty, public services, and the prevention of extremist recruitment?
- 4 How should Nigeria balance the prosecution of suspected terrorists with the rehabilitation and reintegration of former fighters and captives?
- 5 How can the international community protect displaced people, support safe and voluntary returns, and improve humanitarian access to communities affected by armed violence?
- 6 Should the Security Council focus narrowly on Boko Haram and ISWAP, or also address banditry, kidnapping, and communal violence that stretch Nigeria's security forces?
- 7 Are existing sanctions against Boko Haram and ISWAP being enforced effectively, and what additional measures could better disrupt terrorist financing without obstructing humanitarian aid?

TOPIC B

- 1 When should a cyber operation be considered a threat to international peace and security rather than an issue for domestic law enforcement?
- 2 What evidence should be required before the Security Council attributes a cyber operation to a state or non-state actor?
- 3 Should the Security Council create or authorize an independent mechanism to investigate serious cyber operations? How could it remain impartial and protect sensitive information?
- 4 When should the Security Council impose targeted sanctions or other consequences in response to a cyber operation, and how can it avoid escalation based on uncertain attribution?
- 5 How should the international community protect critical civilian infrastructure, including hospitals, power grids, water systems, transportation networks, and emergency communications, from cyber operations?
- 6 How can technologically advanced states and private companies help countries strengthen their cybersecurity without compromising national sovereignty, exposing sensitive data, or creating technological dependence?
- 7 What policies should your country support concerning international law, state responsibility, public attribution, information sharing, and cooperation with private technology companies?

Important Documents

TOPIC A

Global Centre for the Responsibility to Protect. “Nigeria.” Last updated July 15, 2026. www.globalr2p.org/countries/nigeria/.

Human Rights Watch. *Spiraling Violence: Boko Haram Attacks and Security Force Abuses in Nigeria*. New York: Human Rights Watch, October 2012. www.hrw.org/sites/default/files/reports/nigeria1012webwcover_0.pdf.

International Crisis Group. *JAS vs. ISWAP: The War of the Boko Haram Splinters*. Africa Briefing No. 196. Brussels and Dakar: International Crisis Group, March 28, 2024. www.crisisgroup.org/brf/africa/west-africa/nigeria/b196-jas-vs-iswap-war-boko-haram-splinters.

International Crisis Group. *What Role for the Multinational Joint Task Force in Fighting Boko Haram?* Africa Report No. 291. Nairobi and Brussels: International Crisis Group, July 7, 2020. www.crisisgroup.org/rpt/africa/west-africa/291-what-role-multinational-joint-task-force-fighting-boko-haram.

The Soufan Center. “The Islamic State West Africa Province’s Tactical Evolution Fuels Worsening Conflict in Nigeria’s Northeast.” *IntelBrief*, May 21, 2025. thesoufancenter.org/intelbrief-2025-may-21/.

United Nations Office for the Coordination of Humanitarian Affairs. *Nigeria: 2026 Humanitarian Needs and Response Plan*. Abuja: United Nations Office for the Coordination of Humanitarian Affairs, January 22, 2026. www.unocha.org/publications/report/nigeria/nigeria-2026-humanitarian-needs-and-response-plan-january-2026.

United Nations Security Council. Resolution 2349 (2017). S/RES/2349. March 31, 2017. [docs.un.org/S/RES/2349\(2017\)](http://docs.un.org/S/RES/2349(2017)).

TOPIC B

Council of Europe. *Convention on Cybercrime*. European Treaty Series No. 185. November 23, 2001. <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

Council on Foreign Relations. “Cyber Operations Tracker.” Accessed August 16, 2026. <https://www.cfr.org/cyber-operations/>. International Committee of the Red Cross. “The Geneva Conventions and Their Commentaries.” Accessed August 11, 2026. <https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries>.

Multilateral Sanctions Monitoring Team. *The DPRK’s Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities*. October 22, 2025. <https://www.mofa.go.jp/files/100922718.pdf>.

United Nations General Assembly. *Developments in the Field of Information and Telecommunications in the Context of International Security*. A/80/257. July 24, 2025. <https://docs.un.org/en/A/80/257>.

United Nations Office on Drugs and Crime. “United Nations Convention against Cybercrime.” Accessed July 27, 2026. <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

About the Authors

TOPIC A: ALTHEA TURLEY

Althea Turley has studied and worked in West Africa, partnering with local NGOs on initiatives to educate and empower rural communities through human rights, public health, and education. Her experiences in the region sparked a broader interest in the political, humanitarian, and development challenges facing West Africa and the ways in which insecurity can affect communities far beyond the immediate boundaries of a conflict. Althea received her bachelor's and master's degrees in public health in Amherst, Massachusetts. After several years in biotechnology and clinical diagnostics, providing technical training and support to scientific organizations around the world, she transitioned to international education full time. Today, she works for the International Model United Nations Association (IMUNA), developing educational programming and helping students from around the world engage with global issues, diplomacy, and the work of the United Nations. She is particularly passionate about making complex international issues accessible to young people.

TOPIC B: BEA CIRCELLI

Bea Circelli received her Bachelor of Arts in Political Science from Columbia University. She has over a decade of Model UN experience at both the high school and collegiate level, with an International Model United Nations Association (IMUNA) career spanning five years and multiple conferences. Following her time at Columbia, she spent two years working for the New York Legal Assistance Group, a legal nonprofit serving low-income New Yorkers. Currently, she is a second-year law student at Rutgers Law School-Newark, where she aims to work in public interest. As an immigrant and global citizen, she is passionate about human rights, international law, and movement lawyering.

Edited by Adam Allibhoy, Odera Arene, Armen Bagdassarian, Ana Margarita Gil, Aurora Lai, Sabeeh Mirza, and Olivia Woodard

Endnotes

- 1 "Nigeria," CIA World Factbook, accessed 30 August 2026, www.cia.gov/library/publications/the-world-factbook/geos/ni.html
- 2 BBC News, "Nigeria Profile—Timeline," February 18, 2019, www.bbc.com/news/world-africa-13951696.
- 3 Kunle Adebajo and Hamza Ibrahim, "Violent Criminal Gangs Displace and Disrupt North West Nigeria," Africa Center for Strategic Studies, October 21, 2024, africacenter.org/spotlight/spiraling-criminal-gang-violence-in-north-west-nigeria-causing-displacements-and-diminished-government-control/
- 4 "Nigeria," CIA World Factbook.
- 5 Human Rights Watch, *Spiraling Violence*.
- 6 Human Rights Watch, *Spiraling Violence*.
- 7 Human Rights Watch, *Spiraling Violence*.
- 8 Human Rights Watch, "Nigeria," in *World Report 2026: Events of 2025* (New York: Human Rights Watch, 2026), www.hrw.org/world-report/2026/country-chapters/nigeria
- 9 Human Rights Watch, "Nigeria."
- 10 Human Rights Watch, "Nigeria."
- 11 Fabrice Robinet, "Violence Roiling Nigeria Extends Beyond Religious Lines, amid a Deepening Humanitarian Crisis," UN News, January 29, 2026, news.un.org/en/story/2026/01/1166857
- 12 Global Centre for the Responsibility to Protect, "Atrocity Alert No. 487: Sudan, Afghanistan and Nigeria," June 17, 2026, www.globalr2p.org/publications/atrocity-alert-no-487/; Adejumo Kabir, "The Monetisation of Justice by Nigeria's Enforcement Officers," HumAngle, July 3, 2023; Shey Fonjoh Ivo, Angandze Sheily Ngobalep, and Kineh Mirabel Dzelam, "Insurgency: Boko Haram and the Regionalization of Attacks on Education in the Lake Chad Basin, 2000–2025," *International Journal of Research and Innovation in Social Science* 13, no. 6 (June 2026): 812–825, doi. [org/10.51244/IJRISI.2026.1306000055](https://doi.org/10.51244/IJRISI.2026.1306000055).
- 13 Hilary Matfess, "Boko Haram: History and Context," *Oxford Research Encyclopedia of African History*, published October 26, 2017, doi. [org/10.1093/acrefore/9780190277734.013.119](https://doi.org/10.1093/acrefore/9780190277734.013.119)
- 14 Mark Leon Goldberg, "The Baga Massacre," UN Dispatch, 16 January 2015, www.undispatch.com/baga-massacre/.
- 15 ADF, "Report: MNJTF Must Evolve to Contain Terror Threat," Africa Defense Forum, June 9, 2026, adf-magazine.com/2026/06/report-mnjtf-must-evolve-to-contain-terror-threat/
- 16 "Nigeria," CIA World Factbook.
- 17 Ministry of Foreign Affairs, "The People," Federal Republic of Nigeria, accessed 31 August 2026, www.foreignaffairs.gov.ng/nigeria/the-people/.
- 18 Isaac Terwase Sampson, "Religious violence in Nigeria: Causal diagnoses and strategic recommendations to the state and religious communities," *African Journal on Conflict Resolution* 12, No. 1 (2012), www.ajol.info/index.php/ajcr/article/view/78703/69042.
- 19 Sampson, "Religious violence in Nigeria: Causal diagnoses and strategic recommendations to the state and religious communities."
- 20 "Northern Nigeria: Background to Conflict," International Crisis Group, 20 December 2010, www.crisisgroup.org/africa/west-africa/nigeria/northern-nigeria-background-conflict.
- 21 Toyin Falola, *Violence in Nigeria: The Crisis of Religious Politics and Secular Ideologies* (Rochester, NY: University of Rochester Press, 1998), books.google.com/books?id=4X4oYdPpXGQC
- 22 "Nigeria Profile," BBC News, 18 February 2019, www.bbc.com/news/world-africa-13951696.
- 23 "Nigeria Profile," BBC News.
- 24 Isaac Terwase Sampson, "Religious Violence in Nigeria: Causal Diagnoses and Strategic Recommendations to the State and Religious Communities," *African Journal on Conflict Resolution* 12, no. 1 (2012): www.accord.org.za/ajcr-issues/religious-violence-in-nigeria/
- 25 "Spiraling Violence," Human Rights Watch.
- 26 Sampson, "Religious violence in Nigeria."
- 27 Leena Koni Hoffmann and Tommy Hilton, "Corruption in Nigeria," Chatham House, last updated October 3, 2025, www.chathamhouse.org/2025/08/corruption-nigeria
- 28 Oluwafemi Adesina Oyeibanji and Don John Otene Omale, "An Assessment of the Factors of Economic and Financial Corruption by Public Officials in Nigeria," *Journal of Economic Criminology* 10 (2025): 100188, doi.org/10.1016/j.jeconc.2025.100188
- 29 Oyeibanji and Omale, "Factors of Economic and Financial Corruption."
- 30 Dare Ezekiel Arowolo, "Corruption and Counterinsurgency Financing in Nigeria," *Security Science Journal* 6, no. 1 (2025), doi.org/10.37458/ssj.6.1.11.
- 31 Ivo, Ngobalep, and Dzelam, "Insurgency," 812–825.
- 32 Oyeibanji and Omale, "Factors of Economic and Financial Corruption."
- 33 Muhammad Tasiu Dansabo and Usman Ibrahim Dabai, "The Impact of Poverty on Northern Nigeria's Development: A Comprehensive Analysis," *International Journal of Research and Innovation in Social Science* 8, no. 8 (August 2024), doi.org/10.47772/IJRIS.2024.808065
- 34 "Poverty & Equity Brief: Nigeria," World Bank Group, October 2025, documents.worldbank.org/en/publication/documents-reports/documentdetail/099253204222517873
- 35 Eromo Egbejule, "Nigerian Security Forces Free More Than 300 Hostages in 'Largest Single-Day Recovery,'" *The Guardian*, August 6, 2026, www.theguardian.com/world/2026/aug/06/nigerian-security-forces-free-hostages-abducted-by-militants
- 36 Counter Extremism Project, "Abubakar Shekau," accessed August 31, 2026, www.counterextremism.com/extremists/abubakar-shekau.
- 37 "Spiraling Violence," Human Rights Watch.
- 38 "Spiraling Violence," Human Rights Watch.
- 39 Olajumoke Ayandele and Chika Charles Aniekwe, *A Decade After Chibok: Assessing Nigeria's Regional Response to Boko Haram* (ACLED, April 16, 2024), acleddata.com/report/decade-after-chibok-assessing-nigerias-regional-response-boko-haram
- 40 Audu Bulama Bukarti, "The Origins of Boko Haram—and Why It Matters," Hudson Institute, January 13, 2020, www.hudson.org/national-security-defense/the-origins-of-boko-haram-and-why-it-matters.
- 41 Bukarti, "Origins of Boko Haram."
- 42 "Boko Haram," Center for International Security and Cooperation, accessed 2 November 2019, cisac.fsi.stanford.edu/mappingmilitants/profiles/boko-haram; "Spiraling Violence," Human Rights Watch.
- 43 oxfordre.com/africanhistory/view/10.1093/acrefore/9780190277734.001.0001/acrefore-9780190277734-e-119
- 44 Matfess, "Boko Haram: History and Context."
- 45 Bukarti, "Origins of Boko Haram."
- 46 Human Rights Watch, "Nigeria: Boko Haram Attacks Likely Crimes Against Humanity," news release, October 11, 2012, www.hrw.org/

news/2012/10/11/nigeria-boko-haram-attacks-likely-crimes-against-humanity.

47 “Boko Haram,” Center for International Security and Cooperation

48 Human Rights Watch, “Nigeria: Boko Haram Attacks Likely Crimes Against Humanity.”

49 Ivo, Ngobalep, and Dzelam, “Insurgency.”

50 “Spiraling Violence,” Human Rights Watch.

51 Bukarti, “Origins of Boko Haram.”

52 “Spiraling Violence,” Human Rights Watch.

53 Matfess, “Boko Haram: History and Context.”

54 www.counterextremism.com/extremists/abubakar-shekau

55 Bukarti, “Origins of Boko Haram.”

56 Office of the Prosecutor, “Situation in Nigeria Article 5 Report,” International Criminal Court, 5 August 2013, www.legal-tools.org/doc/508bd0/

57 Office of the Prosecutor, “Report on Preliminary Examination Activities 2015,” International Criminal Court, published 12 November 2015, www.icc-cpi.int/sites/default/files/OTP-PE-rep-2015-Eng.pdf.

58 European Asylum Support Office, “1.3.1. Boko Haram, Including JAS, ISWAP and Ansaru,” in Country Guidance: Nigeria (October 2021), www.euaa.europa.eu/country-guidance-nigeria-2021/131-boko-haram-including-jas-iswap-and-ansaru.

59 International Crisis Group, JAS vs. ISWAP: The War of the Boko Haram Splinters, Africa Briefing no. 196 (Brussels and Dakar: International Crisis Group, March 28, 2024), www.crisisgroup.org/brf/africa/west-africa/nigeria/b196-jas-vs-iswap-war-boko-haram-splinters.

60 International Crisis Group, JAS vs. ISWAP.

61 International Crisis Group, JAS vs. ISWAP.

62 UN Security Council, ISIL (Da’esh) and Al-Qaida Sanctions Committee, Islamic State West Africa Province (ISWAP): Narrative Summary of Reasons for Listing, QDe.162 (February 23, 2020), main.un.org/securitycouncil/en/content/islamic-state-west-africa-province-iswap-0.

63 UN Security Council, Islamic State West Africa Province (ISWAP), QDe.162.

64 International Crisis Group, JAS vs. ISWAP.

65 Office of the Prosecutor, “Situation in Nigeria Article 5 Report.”

66 J. Peter Pham, Boko Haram’s Evolving Threat, Africa Security Brief no. 20 (Washington, DC: Africa Center for Strategic Studies, April 30, 2012), africacenter.org/publication/boko-harams-evolving-threat/.

67 David Cook, “Boko Haram Escalates Attacks on Christians in Northern Nigeria,” CTC Sentinel 5, no. 4 (April 2012), ctc.westpoint.edu/boko-haram-escalates-attacks-on-christians-in-northern-nigeria/.

68 Cook, “Boko Haram Escalates Attacks on Christians.”

69 Cook, “Boko Haram Escalates Attacks on Christians.”

70 Cook, “Boko Haram Escalates Attacks on Christians.”

71 Mark Leon Goldberg, “The Baga Massacre,” UN Dispatch, last updated 16 January 2015, www.undispatch.com/baga-massacre/.

72 “Nigeria: Deadliest Boko Haram attack on Rann leaves at least 60 people murdered,” Amnesty International, last updated 1 February 2019, www.amnesty.org/en/latest/news/2019/02/nigeria-deadliest-boko-haram-attack-on-rann-leaves-at-least-60-people-murdered/.

73 “They Set the Classrooms on Fire: Attacks on Education in Northeast Nigeria,” Human Rights Watch, published 2016, www.hrw.org/sites/default/files/report_pdf/nigeria0416web.pdf.

74 “Those Terrible Weeks in Their Camp: Boko Haram Violence against Women and Girls in Northeast Nigeria,” Human Rights Watch, last updated 27 October 2014, www.hrw.org/report/2014/10/27/those-terrible-weeks-their-camp/boko-haram-violence-against-women-and-girls.

75 Human Rights Watch, “Those Terrible Weeks in Their Camp.”

76 Office of the United Nations High Commissioner for Human Rights, “A Decade after Chibok, Nigeria Confronts a New Surge in Child Abductions,” January 12, 2026, www.ohchr.org/en/stories/2026/01/decade-after-chibok-nigeria-confronts-new-surge-child-abductions.

77 Arowolo, “Corruption and Counterinsurgency Financing.”

78 “UN chief condemns abduction of school girls in north-east Nigeria, calls for their immediate release,” UN News, 28 February 2018, news.un.org/en/story/2018/02/1003741

79 UN Security Council, Islamic State West Africa Province (ISWAP), QDe.162.

80 Office of the Prosecutor, “Report on Preliminary Examination Activities 2017,” International Criminal Court, published 4 December 2017, www.icc-cpi.int/171204-rep-otp-PE.

81 International Crisis Group, JAS vs. ISWAP.

82 International Crisis Group, JAS vs. ISWAP.

83 International Crisis Group, JAS vs. ISWAP.

84 Malik Samuel, “When Rebels Rule: ISWAP’s Formula for Winning Support in Nigeria’s Northeast,” The New Humanitarian, July 24, 2025, www.thenewhumanitarian.org/analysis/2025/07/24/when-rebels-rule-iswap-formula-winning-support-nigeria-northeast-tax-control.

85 Human Rights Watch, Spiraling Violence.

86 Amnesty International, Nigeria: Unlawful Killings by the Joint Military Task Force in Maiduguri Must Stop, AFR 44/013/2011 (July 14, 2011), www.amnesty.org/fr/wp-content/uploads/2021/06/afr440132011en.pdf.

87 Human Rights Watch, Spiraling Violence: Boko Haram Attacks and Security Force Abuses in Nigeria (New York: Human Rights Watch, October 2012), www.hrw.org/sites/default/files/reports/nigeria1012webwcover_0.pdf.

88 Human Rights Watch, Spiraling Violence.

89 Human Rights Watch, Spiraling Violence.

90 Global Centre for the Responsibility to Protect, “Atrocity Alert No. 487.”

91 Global Centre for the Responsibility to Protect, “Atrocity Alert No. 487.”

92 Global Centre for the Responsibility to Protect, “Atrocity Alert No. 487.”

93 “New Amnesty Report: Senior Members of Nigerian Military Must be Investigated for War Crimes,” Amnesty International, last updated 2 June 2015, www.amnestyusa.org/press-releases/new-amnesty-report-senior-members-of-nigerian-military-must-be-investigated-for-war-crimes/.

94 “New Amnesty Report: Senior Members of Nigerian Military Must be Investigated for War Crimes,” Amnesty International.

95 Egbejule, “Nigerian Security Forces Free More Than 300 Hostages.”

96 Egbejule, “Nigerian Security Forces Free More Than 300 Hostages.”

97 Egbejule, “Nigerian Security Forces Free More Than 300 Hostages.”

98 Egbejule, “Nigerian Security Forces Free More Than 300 Hostages.”

99 Human Rights Watch, Spiraling Violence.

100 Nnamdi Obasi, “Why Violence Persists in Nigeria: And How Governance Reform Can Break the Cycle,” International Crisis Group, May 13, 2026, www.crisisgroup.org/opd/africa/nigeria/why-violence-persists-nigeria.

101 Obasi, “Why Violence Persists in Nigeria.”

- 102 The Soufan Center, "The Islamic State West Africa Province's Tactical Evolution Fuels Worsening Conflict in Nigeria's Northeast," IntelBrief, May 21, 2025, thesoufancenter.org/intelbrief-2025-may-21/.
- 103 Ogalah Dunamis, "ISWAP Attacks Army Base, Burns Police Post, Public Facilities," Premium Times, July 9, 2026, www.premiumtimesng.com/news/top-news/894000-iswap-attacks-army-base-burns-police-post-public-facilities.html.
- 104 Dunamis, "ISWAP Attacks Army Base, Burns Police Post, Public Facilities."
- 105 Malik Samuel and Ed Stoddard, "Resurgent Jihadist Violence in Northeast Nigeria Part of a Worrying Regional Trend," The New Humanitarian, June 2, 2025, www.thenewhumanitarian.org/analysis/2025/06/02/resurgent-jihadist-violence-northeast-nigeria-part-worrying-regional-trend.
- 106 Eromo Egbejule, "At Least 65 Nigerian Soldiers Killed in Jihadist Raids in Country's North-East," The Guardian, March 11, 2026, www.theguardian.com/world/2026/mar/11/nigerian-soldiers-killed-jihadist-raids-north-east.
- 107 Human Rights Watch, "Nigeria."
- 108 The Soufan Center, "The Islamic State West Africa Province's Tactical Evolution Fuels Worsening Conflict in Nigeria's Northeast," IntelBrief, May 21, 2025, thesoufancenter.org/intelbrief-2025-may-21/.
- 109 The Soufan Center, "ISWAP's Tactical Evolution."
- 110 Jacob Zenn, "Boko Haram Pledges Loyalty to Mysterious New Leader: Abu Umamata," Militant Leadership Monitor, The Jamestown Foundation, June 6, 2022, jamestown.org/brief/boko-haram-pledges-loyalty-to-mysterious-new-leader-abu-umamata/.
- 111 Jacob Zenn, "Brief: Boko Haram Leader Allegedly Killed in Nigerian Airstrike," Terrorism Monitor 23, no. 6 (September 20, 2025), jamestown.org/brief-boko-haram-leader-allegedly-killed-in-nigerien-airstrike/.
- 112 Samuel, "When Rebels Rule."
- 113 Samuel, "When Rebels Rule."
- 114 Samuel, "When Rebels Rule."
- 115 Chinedu Asadu, "What to Know as Nigeria Rejects U.S. Military Threat over Alleged Christian Killings," Associated Press, November 2, 2025, apnews.com/article/nigeria-trumo-christians-persecution-2aa6ffc42eeedc260122021bf51b0028.
- 116 Asadu, "Nigeria Rejects U.S. Military Threat."
- 117 Luka Binniyat and Sulieman Ayuba, "40 Children Abducted as Boko Haram Kills Eight in Borno," Genocide Watch, May 17, 2026, www.genocidewatch.com/single-post/40-children-abducted-as-boko-haram-kills-eight-in-borno.
- 118 Binniyat and Ayuba, "40 Children Abducted."
- 119 Raoul Sumo Tayo, "Will the U.S.-Nigeria Targeting of ISWAP's Deputy Weaken Terrorism?" ISS Today, May 27, 2026, issafrica.org/iss-today/will-the-us-nigeria-targeting-of-iswap-s-deputy-weaken-terrorism.
- 120 Tayo, "Will the U.S.-Nigeria Targeting of ISWAP's Deputy Weaken Terrorism?"
- 121 Tayo, "Will the U.S.-Nigeria Targeting of ISWAP's Deputy Weaken Terrorism?"
- 122 International Crisis Group, "Nigeria," CrisisWatch: July Trends and August Alerts 2026, accessed September 2, 2026, www.crisisgroup.org/crisiswatch/july-trends-and-august-alerts-2026#nigeria.
- 123 International Crisis Group, "Nigeria."
- 124 Global Centre for the Responsibility to Protect, "Nigeria,"
- 125 Scholastica Hir, "Benue PDP, Muftwang Reject Description of Insecurity as Farmer-Herder Clashes," The Sun, September 1, 2026, thesun.ng/benue-pdp-muftwang-reject-description-of-insecurity-as-farmer-herder-clashes/.
- 126 International Crisis Group, "Nigeria."
- 127 Sallek-Yaks Musa, "Banditry and Modern Slavery: (In)security Dynamics in Nigeria," Journal of Economic Criminology 10 (October 2025): 1–9, doi.org/10.1016/j.jeconc.2025.100194.
- 128 Musa, "Banditry and Modern Slavery."
- 129 Musa, "Banditry and Modern Slavery."
- 130 James Barnett and Umar Musa, "Kachallas and Kinship: Understanding Jihadi Expansion and Diffusion in Nigeria," CTC Sentinel 19, no. 1 (January 2026), ctc.westpoint.edu/kachallas-and-kinship-understanding-jihadi-expansion-and-diffusion-in-nigeria/.
- 131 Global Centre for the Responsibility to Protect, "Atrocity Alert No. 487."
- 132 Global Centre for the Responsibility to Protect, "Atrocity Alert No. 487."
- 133 Agence France-Presse, "Nigerian Armed Groups Net Nearly \$6 Million in Ransoms: Study," RTL Today, August 26, 2026, today.rtl.lu/news/world/nigerian-armed-groups-net-nearly-6-mn-in-ransoms-study-1681384389.
- 134 France-Presse, "Nigerian Armed Groups Net Nearly \$6 Million."
- 135 Fatai Alli, Revitalizing Integrated Tactical Units to Combat West Africa's Irregular Militant Groups, Africa Security Brief no. 47 (Washington, DC: Africa Center for Strategic Studies, February 9, 2026), africacenter.org/publication/asb47en-integrated-tactical-units-west-africa/.
- 136 United Nations Development Programme, "1.1 Million Lives Highly at Risk in North-East Nigeria by 2030 if Development Deficit Continues, Says UNDP Report," news release, June 23, 2021, www.undp.org/nigeria/press-releases/11-million-lives-highly-risk-north-east-nigeria-2030-if-development-deficit-continues-says-undp-report.
- 137 Simone Papale and Emanuele Castelli, "Food, Terrorism, and the Boko Haram and Al-Shabaab Insurgencies," Studies in Conflict & Terrorism (February 3, 2025): 1–25, doi.org/10.1080/1057610X.2025.2457427.
- 138 European Commission, "Nigeria," European Civil Protection and Humanitarian Aid Operations, last updated April 21, 2026, civil-protection-humanitarian-aid.ec.europa.eu/where/africa/nigeria_en.
- 139 European Commission, "Nigeria."
- 140 European Commission, "Nigeria."
- 141 United Nations Office for the Coordination of Humanitarian Affairs, Nigeria: 2026 Humanitarian Needs and Response Plan (Abuja: United Nations Office for the Coordination of Humanitarian Affairs, January 22, 2026), www.unocha.org/publications/report/nigeria/nigeria-2026-humanitarian-needs-and-response-plan-january-2026.
- 142 Amnesty International, "Nigeria: Girls Failed by Authorities after Escaping Boko Haram Captivity—New Report," news release, June 9, 2024, www.amnesty.org/en/latest/news/2024/06/nigeria-girls-failed-by-authorities-after-escaping-boko-haram-captivity-new-report/.
- 143 Amnesty International, "Girls Failed by Authorities."
- 144 Amnesty International, "Girls Failed by Authorities."
- 145 Mary Crickmore, "The Role of Christian Ethnic Militias in Nigeria's Violence," Baptist News Global, August 31, 2026, baptistnews.com/article/the-role-of-christian-ethnic-militias-in-nigerias-violence/.
- 146 Crickmore, "The Role of Christian Ethnic Militias."
- 147 National Human Rights Commission of Nigeria, "Refugees and Displaced Persons Deserve Dignity and Protection," June 20, 2025, nigeriarights.gov.ng/nhrc-media/news-and-events/563-refugees-and-displaced-persons-deserve-dignity-and-protection-nhrc.html.
- 148 S. D. Nashut, "Ranching, Land and the Soul of Nigeria," Sundiatapost, August 28, 2026, sundiatapost.com/ranching-land-and-the-soul-of-nigeria/.

-
- 149 National Human Rights Commission of Nigeria, "Refugees and Displaced Persons."
- 150 National Human Rights Commission of Nigeria, "Refugees and Displaced Persons."
- 151 Nashut, "Ranching, Land and the Soul of Nigeria."
- 152 Rita Iorbo et al., "Social Inclusion and Justice for the Internally Displaced by the Herdsmen-Farmers Conflict in Benue State, Nigeria," *Journal on Migration and Human Security* 12, no. 2 (June 2024): 96–109, doi.org/10.1177/23315024241239585.
- 153 Peter Duru, "Benue Leaders Reject FG Ranching Plan, Demand IDPs' Return," *Vanguard News*, August 14, 2026, www.vanguardngr.com/2026/08/benue-leaders-reject-fg-ranching-plan-demand-idps-return/.
- 154 OHCHR, "A Decade after Chibok."
- 155 OHCHR, "A Decade after Chibok."
- 156 National Human Rights Commission of Nigeria, "Refugees and Displaced Persons."
- 157 Camillus Eboh and Elisha Bala-Gbogbo, "Nigeria to Lead Humanitarian Response as UN Support Evolves, Minister Says," *Reuters*, July 14, 2026, www.reuters.com/world/africa/nigeria-lead-humanitarian-response-un-support-evolves-minister-says-2026-07-14/.
- 158 United Nations Office for the Coordination of Humanitarian Affairs, "Nigeria Humanitarian Needs and Response Plan 2026," *Financial Tracking Service*, accessed September 2, 2026, fts.unocha.org/plans/1508/summary.
- 159 Eboh and Bala-Gbogbo, "Nigeria to Lead Humanitarian Response."
- 160 Global Centre for the Responsibility to Protect, "Nigeria."
- 161 Global Centre for the Responsibility to Protect, "Nigeria."
- 162 Global Centre for the Responsibility to Protect, "Nigeria."
- 163 Daniel Williams, "Nigerians Caught in the Crossfire," *Washington Post*, October 11, 2012, www.hrw.org/news/2012/10/11/nigerians-caught-crossfire.
- 164 Global Centre for the Responsibility to Protect, "Nigeria."
- 165 Human Rights Watch, "Spiraling Violence: Boko Haram Attacks and Security Force Abuses in Nigeria."
- 166 Ayandele and Aniekwe, *A Decade After Chibok*.
- 167 Ayandele and Aniekwe, *A Decade After Chibok*.
- 168 Ayandele and Aniekwe, *A Decade After Chibok*.
- 169 Global Centre for the Responsibility to Protect, "Nigeria."
- 170 ADF, "MNJTF Must Evolve."
- 171 Multinational Joint Task Force, "Civil-Military Cooperation," accessed September 2, 2026, mnjtfmm.org/cimic/.
- 172 Multinational Joint Task Force, "Civil-Military Cooperation."
- 173 ADF, "MNJTF Must Evolve."
- 174 International Crisis Group, *What Role for the Multinational Joint Task Force in Fighting Boko Haram?*, Africa Report no. 291 (Nairobi and Brussels: International Crisis Group, July 7, 2020), www.crisisgroup.org/rpt/africa/west-africa/291-what-role-multinational-joint-task-force-fighting-boko-haram
- 175 International Crisis Group, *What Role for the Multinational Joint Task Force?*
- 176 ADF, "MNJTF Must Evolve."
- 177 ADF, "MNJTF Must Evolve."
- 178 ADF, "MNJTF Must Evolve."
- 179 United Nations High Commissioner for Refugees, *Lake Chad Basin Regional Protection and Displacement Crisis: Humanitarian Priorities and Funding Needs across Cameroon, Chad, Niger and Nigeria*, June–December 2026 (Geneva: UNHCR, June 2026), reliefweb.int/report/cameroon/lake-chad-basin-regional-protection-and-displacement-crisis-humanitarian-priorities-and-funding-needs-across-cameroon-chad-niger-and-nigeria-june-december-2026
- 180 UNHCR, *Lake Chad Basin Regional Protection and Displacement Crisis*.
- 181 UN Security Council, *Draft Resolution, S/2017/270* (March 31, 2017), digitallibrary.un.org/record/863829/files/S_2017_270-EN.pdf.
- 182 United Nations Office of Counter-Terrorism, "Partnership with the Counter-Terrorism Committee Executive Directorate," *United Nations Global Counter-Terrorism Coordination Compact*, accessed September 2, 2026, www.un.org/counterterrorism/en/global-ct-compact/partnership-CTED.
- 183 UN Security Council, *Islamic State West Africa Province (ISWAP)*, QDe.162.
- 184 BBC News Pidgin, "Nigeria publish list of suspected sponsors of terrorism," *BBC News Pidgin*, 11 April 2026, www.bbc.com/pidgin/articles/cg40exrne0yo
- 185 Basit Jamui, "Things to Know About Individuals on FG's Sanctioned List of Terrorism Financiers in 2026," *Legit.ng*, April 13, 2026, www.legit.ng/nigeria/1705215-things-individuals-fgs-sanctioned-list-terrorism-financiers-2026/.
- 186 BBC News Pidgin, "Nigeria publish list of suspected sponsors of terrorism,"
- 187 Chainalysis Team, "Asset Seizure and Cryptocurrency: How Chainalysis Creates Opportunities for Self-Sustaining Law Enforcement," *Chainalysis*, March 26, 2025, www.chainalysis.com/blog/cryptocurrency-asset-seizure/.
- 188 France-Presse, "Nigerian Armed Groups Net Nearly \$6 Million."
- 189 U.S. Department of State, Bureau of Political-Military Affairs, "U.S. Security Cooperation with Nigeria," fact sheet, January 23, 2024, www.state.gov/u-s-security-cooperation-with-nigeria.
- 190 United Nations Development Programme, "Launch of the New Phase of the Regional Stabilization Facility for the Lake Chad Basin," news release, July 30, 2024, www.undp.org/africa/waca/press-releases/launch-new-phase-regional-stabilization-facility-lake-chad-basin-0.
- 191 United Nations in Nigeria, "UN Entities in Nigeria," accessed September 2, 2026, nigeria.un.org/en/about/un-entities-in-country
- 192 Ayandele and Aniekwe, *A Decade After Chibok*.
- 193 Laura Sharman, "US and Nigerian forces kill senior ISIS commander, Trump says," *CNN*, May 16, 2026, https://www.cnn.com/2026/05/16/africa/us-nigeria-isis-commander-killed-intl-hnk.
- 194 Boubba Jalloh, "Nigeria expands security ties amid insurgency," *DSW*, March 25, 2026, https://www.dw.com/en/nigeria-moves-to-broaden-security-alliances-amid-ongoing-insurgency-threats/a-76512959.
- 195 Sertan Sanderson, "UK–Nigeria relations in focus as London hosts Tinubu," *DSW*, March 3, 2019, https://www.dw.com/en/uknigeria-relations-in-focus-as-london-hosts-tinubu/a-76424268.
- 196 "China Warns US Against Interfering In Nigeria's Affairs After Trump's Military Threat," *Arise News*, November 4, 2025, https://www.arise.tv/china-warns-us-against-interfering-in-nigerias-affairs-after-trumps-military-threat/.
- 197 "Russia, AU Tell US To Respect Nigeria's Sovereignty Amid Talk Of Possible Military Action," *Arise News*, November 8, 2025, https://www.arise.tv/russia-au-tell-us-to-respect-nigerias-sovereignty-amid-talk-of-possible-military-action/.
- 198 UN Security Council, *Draft Resolution, S/2017/270* (March 31, 2017), digitallibrary.un.org/record/863829/files/S_2017_270-EN.pdf.
- 199 "UN Security Council Informal Group visits Nigeria, addresses Climate, Peace, and Security Challenges in Lake Chad basin," *United Nations*,

- accessed September 6, 2026, <https://www.un.org/climatesecuritymechanism/en/news/un-security-council-informal-group-visits-nigeria-addresses-climate-peace-and-security>.
- 200 "Cyber Operations Tracker," Council on Foreign Relations, accessed August 16, 2026, <https://www.cfr.org/cyber-operations/>.
- 201 Theo Leggett, "Jaguar Land Rover posts heavy loss after cyber-attack," BBC, November 14, 2025, accessed July 27, 2026, <https://www.bbc.com/news/articles/ckg1w255gy1o>.
- 202 "What Is Cybercrime?," Cisco, accessed August 22, 2026, <https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html>.
- 203 "Cyber Terrorism," Wigan Council, accessed August 22, 2026, <https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx>.
- 204 "Cybersecurity," U.S. Government Accountability Office, accessed August 10, 2026, <https://www.gao.gov/cybersecurity>.
- 205 "What Is Cybersecurity?," Cybersecurity and Infrastructure Security Agency, accessed August 10, 2026, <https://www.cisa.gov/news-events/news/what-cybersecurity>.
- 206 Jennifer Cawthra et al., *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*, NIST Special Publication 1800-26A, vol. A, Executive Summary (National Institute of Standards and Technology, December 2020), <https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html>.
- 207 "A Brief History of Computer Viruses & What the Future Holds," Kaspersky, accessed August 10, 2026, <https://usa.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>.
- 208 Richard Schantz, "Distributed Computing at BBN," in *A Culture of Innovation: Insider Accounts of Computing and Life at BBN*, ed. David Walden and Raymond Nickerson (East Sandwich, MA: Waterside Publishing, 2011), 452.
- 209 Kaspersky, "A Brief History of Computer Viruses."
- 210 "A short history of the internet," Science and Media Museum, 3 December 2020, <https://www.scienceandmediamuseum.org.uk/objects-and-stories/short-history-internet>.
- 211 "A short history of the internet."
- 212 Apisada Suwansukroj, "Annual Meeting on Cybersecurity 2026: The Rise of Cybersecurity as a Strategic Economic Priority," World Economic Forum, May 15, 2026, <https://www.weforum.org/stories/cybersecurity/cybersecurity-systemic-economic-and-strategic-imperative/>.
- 213 Suwansukroj, "Rise of Cybersecurity as a Strategic Economic Priority."
- 214 "Morris Worm," Federal Bureau of Investigation, accessed August 10, 2026, <https://www.fbi.gov/history/cases-and-criminals/morris-worm>.
- 215 U.S. Department of Justice, "9-48.000 - Computer Fraud and Abuse Act," Justice Manual, updated May 2022, <https://www.justice.gov/jm/jm-9-48000-computer-fraud>.
- 216 Data Protection Act 1984, c. 35 (UK), <https://www.legislation.gov.uk/ukpga/1984/35/contents>.
- 217 Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," Nautilus Institute for Security and Sustainability, December 10, 1999, accessed August 15, 2026, <https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/>.
- 218 "Hacker Ethics," Chaos Computer Club, accessed August 15, 2026, <https://www.ccc.de/en/hackerethik>.
- 219 Elizabeth Rhoetter Purdy, "Anonymous," EBSCO Research Starters, 2024, accessed July 27, 2026, <https://www.ebsco.com/research-starters/biography/anonymous>.
- 220 Purdy, "Anonymous."
- 221 "What Is Ethical Hacking," EC-Council, January 19, 2024, <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-ethical-hacking/>.
- 222 Oliver Knight, "How Ethical Hackers with Just a \$3,000 Server Found a Flaw That Could've Put \$70 Billion in Crypto at Risk," CoinDesk, July 4, 2026, accessed August 12, 2026, <https://www.coindesk.com/tech/2026/07/04/how-ethical-hackers-with-just-a-usd3-000-server-found-a-flaw-that-could-ve-put-usd70-billion-in-crypto-at-risk>.
- 223 "Cybersecurity: Social Engineering," Council of the European Union, last reviewed February 5, 2025, accessed August 19, 2026, <https://www.consilium.europa.eu/en/policies/cybersecurity-social-engineering/>.
- 224 "Phishing attacks – who is most at risk?" Office for National Statistics, September 26, 2022, <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/phishingattackswhoismostatrisk/2022-09-26>.
- 225 "What Is a DDoS Attack?" Microsoft Security, accessed August 8, 2026, <https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack>.
- 226 "Risks and Challenges," Council of Europe, accessed August 4, 2026, <https://www.coe.int/en/web/ransomware/risks-and-challenges>.
- 227 "Deepfakes, voice cloning and weaponised AI: Global wake-up call to organised fraud," UN News, March 17, 2026, <https://news.un.org/en/story/2026/03/1167144>.
- 228 "Spoofing and Phishing," FBI, accessed July 31, 2026, <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing>.
- 229 "Spoofing and Phishing."
- 230 "Spyware," US-CERT, accessed August 14, 2026, https://www.cisa.gov/sites/default/files/publications/spywarehome_0905.pdf.
- 231 "What Is a Trojan Horse? Trojan Virus and Malware Explained," Fortinet, accessed August 6, 2026, <https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus>.
- 232 Chris Johnson, Lee Badger, David Waltermire, Julie Snyder, and Clem Skorupka, *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150 (National Institute of Standards and Technology, October 2016), accessed August 17, 2026, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>.
- 233 "What Is Malware?," IBM Think.
- 234 Saman Iftikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures," *PeerJ Computer Science* 10 (2024): e1772, accessed August 11, 2026, <https://pmc.ncbi.nlm.nih.gov/articles/PMC10803091/>.
- 235 "Cyber Operations Tracker."
- 236 "Cyber Operations Tracker."
- 237 "Cyber-attacks on critical infrastructure," Allianz Commercial, April 2026, <https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-attacks-on-critical-infrastructure.html>.
- 238 James Coker, "Russian Hacking Group Sandworm Linked to Unprecedented Attack on Danish Critical Infrastructure," *Infosecurity Magazine*, November 16, 2023, accessed August 5, 2026, <https://www.infosecurity-magazine.com/news/russian-sandworm-attack-danish/>.
- 239 Connor Jones, "EU and UK officially blame Russian spies for cyberattack on Poland's power grid," *The Register*, July 13, 2026, accessed August 18, 2026, <https://www.theregister.com/security/2026/07/13/uk-eu-officially-pin-poland-energy-cyberattack-on-russia/5270458/>.
- 240 Jones, "EU and UK officially blame Russian spies for cyberattack on Poland's power grid."
- 241 Iftikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures."
- 242 "Targeting of Google Chrome users in the United States, South Korea, and Europe," Council on Foreign Relations, June 2024, <https://>

www.cfr.org/cyber-operations/targeting-of-google-chrome-users-in-the-united-states-south-korea-and-europe-particularly-those-involved-in-research-into-north-korean-affairs.

243 "Targeting of foreign embassies in Kyiv," Council on Foreign Relations, September 2023, <https://www.cfr.org/cyber-operations/targeting-of-foreign-embassies-in-kyiv>.

244 "Targeting of Uyghurs Outside China with Trojanized Signal and Telegram Apps," Council on Foreign Relations, accessed July 20, 2026, <https://www.cfr.org/cyber-operations/targeting-of-uyghurs-outside-china-with-trojanized-signal-and-telegram-apps>.

245 Ifitikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures."

246 "Cyberterrorism," UNODC Teaching Module Series: Cybercrime, United Nations Office on Drugs and Crime, accessed August 9, 2026, <https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/cyberterrorism.html>.

247 Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND Corporation, 2001), 239–44.

248 Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy."

249 Vinay Lal, "Terror and Its Networks: Disappearing Trails in Cyberspace," *Global Problem Solving*, April 25, 2002, <https://nautilus.org/global-problem-solving/terror-and-its-networks-disappearing-trails-in-cyberspace/>.

250 "We're Being Played through Propaganda, Memes, and War," *Psychology Today*, accessed August 19, 2026, <https://www.psychologytoday.com/us/blog/positively-media/202604/were-being-played-through-propaganda-memes-and-war>.

251 Denning, "Activism, Hacktivism, and Cyberterrorism."

252 "Why Disinformation Is a Cybersecurity Threat," EU DisinfoLab, May 24, 2021, <https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/>.

253 Multilateral Sanctions Monitoring Team, *The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities*, October 22, 2025, <https://www.mofa.go.jp/files/100922718.pdf>.

254 Ifitikhar, "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures."

255 United Nations, "United Nations Charter (full text)," United Nations, accessed August 26, 2026, <https://www.un.org/en/about-us/un-charter/full-text>.

256 "Use of force," *International Cyber Law: Interactive Toolkit*, NATO Cooperative Cyber Defence Centre of Excellence, accessed August 26, 2026, https://cyberlaw.ccdcoe.org/wiki/Use_of_force#cite_note-14.

257 United Nations General Assembly, "Combating the Criminal Misuse of Information Technologies," United Nations General Assembly Resolution 55/63, adopted December 4, 2000, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf.

258 Council of Europe, "Convention on Cybercrime," *European Treaty Series—No. 185*, November 23, 2001, <https://www.europarl.europa.eu/cms-data/179163/20090225ATT50418EN.pdf>.

259 "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols," Council of Europe, accessed August 14, 2026, <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

260 United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/80/257, July 24, 2025, <https://docs.un.org/en/A/80/257>.

261 *Developments in the Field of Information and Telecommunications in the Context of International Security*.

262 "United Nations Convention against Cybercrime," United Nations Office on Drugs and Crime, accessed July 27, 2026, <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>.

263 Vibhu Mishra, "Sixty-Five Nations Sign First UN Treaty to Fight Cybercrime, in Milestone for Digital Cooperation," *UN News*, October 25, 2025, <https://news.un.org/en/story/2025/10/1166182>.

264 "Cybersecurity and New Technologies," United Nations Office of Counter-Terrorism, accessed August 3, 2026, <https://www.un.org/counterterrorism/en/cct/programme-projects/cybersecurity>.

265 "Ministry of Foreign Affairs Co-hosts the International Conference on the Global Partnership against Online Scams," Ministry of Foreign Affairs, Kingdom of Thailand, December 29, 2025, <https://www.mfa.go.th/en/content/global-partnership-against-online-scams-en>.

266 "Ministry of Foreign Affairs Co-hosts the International Conference on the Global Partnership against Online Scams."

267 "The Geneva Conventions and Their Commentaries," International Committee of the Red Cross, accessed August 11, 2026, <https://www.icrc.org/en/law-and-policy/geneva-conventions-and-their-commentaries>.

268 Tomáš Minárik and Kris van der Meij, "Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention,'" NATO Cooperative Cyber Defence Centre of Excellence, July 18, 2017, <https://ccdcoe.org/news/2017/geneva-conventions-apply-to-cyberspace-no-need-for-a-digital-geneva-convention/>.

269 Kuheli Raha Roy, "How State Sponsored Cyber Attacks Are Changing the Global Threat Landscape," *Fidelis Security*, June 1, 2026, <https://fidelissecurity.com/cybersecurity-101/cyberattacks/state-sponsored-attack/>.

270 "Nation-State Cyber Warfare: How Cybersecurity Professionals Defend the New Digital Battlefield," *Capitol Technology University*, November 3, 2025, <https://www.captechu.edu/blog/how-cybersecurity-professionals-defend-the-new-digital-battlefield>.

271 Martin Hinton, "2025 Cybersecurity Trends: AI, Ransomware, and Cyberattack Surge," *Cyber Insurance News*, January 20, 2025, <https://cyberinsurancenews.org/2025-cybersecurity-trends/>.

272 "AI Has Made Phishing Worse, and Here's What to Do About It," *NINJIO*, July 14, 2026, <https://ninjio.com/blog/ai-has-made-phishing-worse/>.

273 Ramón Reichert, "Autonomous Occupation: Israel's AI-Driven Drone Warfare and the Digital Architecture of Authoritarian Power," *Dialogues on Digital Society* 1, no. 3 (2025): 368–72, <https://doi.org/10.1177/29768640251381423>.

274 Reichert, "Autonomous Occupation: Israel's AI-Driven Drone Warfare and the Digital Architecture of Authoritarian Power."

275 Reichert, "Autonomous Occupation: Israel's AI-Driven Drone Warfare and the Digital Architecture of Authoritarian Power."

276 "When Ransomware Kills: Attacks on Healthcare Facilities," *IBM*, March 12, 2025, <https://www.ibm.com/think/insights/when-ransomware-kills-attacks-on-healthcare-facilities>.

277 Martin Hinton, "2025 Cybersecurity Trends: AI, Ransomware, and Cyberattack Surge," *Cyber Insurance News*, January 20, 2025, <https://cyberinsurancenews.org/2025-cybersecurity-trends/>.

278 "Synnovis Cyber Incident," *NHS England*, last updated November 10, 2025, <https://www.england.nhs.uk/synnovis-cyber-incident/>.

279 "When Ransomware Kills: Attacks on Healthcare Facilities."

280 "Baby Died Due to Ransomware Attack on Hospital, Lawsuit Claims," *NBC News*, accessed August 18, 2026, <https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465>.

281 "Canvas Data Breach: What Students, Parents, and Faculty Need to Know," *National Cybersecurity Alliance*, May 26, 2026, <https://www.staysafeonline.org/articles/canvas-data-breach>.

282 Michael Wilner, "Iran Attempting Cyberattacks against Critical U.S. Infrastructure, Officials Say," *Los Angeles Times*, April 7, 2026, <https://www.latimes.com/politics/story/2026-04-07/iran-attempting-cyber-attacks-against-u-s-critical-infrastructure-officials-say>.

283 Wilner, "Iran Attempting Cyberattacks against Critical U.S. Infrastructure, Officials Say."

-
- 284 Zane Irwin, "Water Plants Under Fire in the Gulf Are Crucial to Civilians," *New York Times*, July 21, 2026, <https://www.nytimes.com/2026/07/21/world/middleeast/desalination-water-middle-east.html>.
- 285 John Raffensperger, "Why Are Cyberattacks a Major Threat to Energy Companies?" *GE Vernova*, 2021, <https://www.gevernova.com/gas-power/resources/articles/2021/energy-cyber-attack>.
- 286 Doney Abraham, Siv Hilde Houmb, and Laszlo Erdodi, "Cyber-Attacks on Energy Infrastructure—A Literature Overview and Perspectives on the Current Situation," *Applied Sciences* 15, no. 17 (2025): 9233, <https://doi.org/10.3390/app15179233>.
- 287 Anna Ribeiro, "CERT Polska Exposes Multi-Stage Cyberattack on Energy Infrastructure Involving VPN, Private APN, OT Network Tunneling," *Industrial Cyber*, August 12, 2026, <https://industrialcyber.co/utilities-energy-power-water-waste/cert-polska-exposes-multi-stage-cyberattack-on-energy-infrastructure-involving-vpn-private-apn-ot-network-tunneling/>.
- 288 Alexander Martin, "Poland Uncovers Second Heat Plant Cyberattack That Went Hidden for Months," *The Record*, August 10, 2026, <https://therecord.media/poland-uncovers-critical-infrastructure-attack-hidden>.
- 289 Naveen Goud, "Ransomware Attack Disrupts Hospital Doors, Elevators, Ventilation and Air Conditioning in Canada," *Cybersecurity Insiders*, August 11, 2026, <https://www.cybersecurity-insiders.com/ransomware-attack-disrupts-hospital-doors-elevators-ventilation-and-air-conditioning-in-canada/>.
- 290 James, "14 Recent Cyber Attacks on the Transport & Logistics Sector," *Wisdiam*, September 29, 2024, <https://wisdiam.com/publications/recent-cyber-attacks-transport-logistics-sector/>.
- 291 James, "14 Recent Cyber Attacks on the Transport & Logistics Sector."
- 292 James, "14 Recent Cyber Attacks on the Transport & Logistics Sector."
- 293 Universal Declaration of Human Rights, United Nations, December 10, 1948, <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.
- 294 "The Protection of Hospitals during Armed Conflicts: What the Law Says," International Committee of the Red Cross, November 6, 2023, <https://www.icrc.org/en/document/protection-hospitals-during-armed-conflicts-what-law-says>.
- 295 Andrew C. Adams and Daniel Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention," *Lawfare*, December 9, 2024, <https://www.lawfaremedia.org/article/confusion---contradiction-in-the-un--cybercrime--convention>.
- 296 Adams and Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention."
- 297 Adams and Podair, "Confusion & Contradiction in the UN 'Cybercrime' Convention."
- 298 "The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be," U.S. Government Accountability Office, August 29, 2023, <https://www.gao.gov/blog/u.s.-less-prepared-fight-cybercrime-it-could-be>.
- 299 Jake Sepich, "The Evolution of Cyber Attribution," *American University*, April 19, 2023, <https://www.american.edu/sis/centers/security-technology/the-evolution-of-cyber-attribution.cfm>.
- 300 "Obstacles to Cybercrime Investigations," United Nations Office on Drugs and Crime, accessed August 7, 2026, <https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html>.
- 301 Sepich, "The Evolution of Cyber Attribution."
- 302 "The U.S. Is Less Prepared to Fight Cybercrime Than It Could Be."
- 303 Nishchal Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges," *Journal of Forensic, Legal & Investigative Sciences* 11 (2025): 105, <https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technological-advancements-and-future-challenges>.
- 304 Soni, "Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges."
- 305 Ben Wolford, "What Is GDPR, the EU's New Data Protection Law?," *GDPR*, accessed August 25, 2026, <https://gdpr.eu/what-is-gdpr/>.
- 306 Stanford University, "China's Great Firewall," *Free Speech vs. Maintaining Social Cohesion: A Closer Look at Different Policies*, 2011, https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html.
- 307 "Developing Countries Most Vulnerable to Cyberattacks – UN," *UN News*, December 9, 2011, <https://news.un.org/en/story/2011/12/397922>.
- 308 "What Is the Security Council?," United Nations Security Council, accessed August 25, 2026, <https://main.un.org/securitycouncil/en/content/what-security-council>.
- 309 "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression," United Nations Charter, accessed August 25, 2026, <https://www.un.org/en/about-us/un-charter/chapter-7>.
- 310 "Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression."

The National High School Model United Nations Conference (NHSMUN) is a project of IMUNA, a non-profit organization formally associated with the United Nations Department of Global Communications (UNDGC). IMUNA is dedicated to promoting global issues education through simulation.

© 2026 IMUNA. All Rights Reserved.

